Internet Policy Report
Brazil 2011

observatório da internet .br
brazilian observatory for digital policies

FGV DIREITO RIO • cts

cgi.br
Brazilian Internet Steering Committee

Internet Policy Report
Brazil 2011

observatório da internet .br
brazilian observatory for digital policies

DIREITO RIO
• cts

Brazilian Internet Steering Committee

Editor in chief
Bruno Magrani

Researchers in charge of the survey and content of this annual publication:

CTS-FGV
Bruno Magrani, Carlos Affonso Pereira de Souza, Eduardo Magrani, Giovanna Carloni, Koichi Kameda, Marília Maciel, Marília Monteiro, Pedro Augusto Francisco, Ronaldo Lemos and Walter Britto.

CGI.br / NIC.br
Vagner Diniz (W3C Brasil), Caroline Burle (W3C Brasil), Crisitne Hoepers (Cert.br), Klaus Steding-Jessen (Cert.br), Alexandre Barbosa (CETIC.br), Antonio Marcos Moreiras (CEPTRO.br), Eduardo Ascenço Reis (PTT|Metro.br) and Fabrício Tamusiunas (SIMET.br).

Presentation

The origin of the Brazilian Internet Steering Committee – CGI.br dates back to 1995, when the Internet and the Web in Brazil comprised only a few thousand domains and no more than a handful of councilors sat on the committee. Since then, it has expanded beyond anything imaginable at the time. The time span itself is relatively short – barely 20 years of CGI.br history. But it is millions of domains later. We are also many additional councilors. Many have sat on the committee in previous terms. And many are the seats occupied by the current 21 councilors, representing different sectors.

I am rightly proud to have been an active participant of this history, sharing dreams and achievements with many others who, since the beginning, have joined in forming a network which is multisectorial, multiparticipative, multilateral, or even multistakeholder, as the governance model for plural organisms and multiple interests is nowadays know.

Indeed, if there is anything in today's multiple world that deserves to be called plural, interactive, participative and collaborative, it is the Internet and the Web. We creatively reference links in ways we could never have predicted before. We research and observe such abundant and diverse information that we are unable to fathom how massive is the quantity of documents, objects, applications and services accessible through our browsing devices.

For what it represents, and maybe for even more, we have intensified talks and debates in order to develop policies and legislation related to this new dimension of social interaction: living online in the Brazilian Internet. Our discussions have been guided by the observation of the principles, rights and obligations of using the Brazilian internet. Therefore, the association between the CGI.br and the Center for Technology and Society of the Law School of the Getúlio Vargas Foundation of Rio de Janeiro (CTS-FGV) could not have been more opportune.

Together, we have created the Brazilian Observatory for Digital Policies or, as it has become known, the Brazilian Internet Observatory.

It is not really just a happy coincidence, since we are participants and designers of these new network modes. But we converge in our aim and acknowledgment of the need for observation. Permanent observation and analysis of the main Internet regulation initiatives. Observation and comparison of international proposals, of Internet steering models.

The current publication is the result of the first joint observations carried out by the CGI.br and the CTS/FGV. We have given it the title of "Internet Policy Report – Brazil 2011" and in it we discourse on the bills and debates which arose in 2011 related to attempts to legislate on Internet crime, to disciplining principles and rights via the Internet Regulatory Framework, to network neutrality, to broadband, to measuring quality and many other topics.

This is the first systematized publication of the Brazilian Internet Observatory. It will not be the last. Its actual reading will inspire new analyses and investigations. We are still very young. The CGI.br is barely 20 years old and there is still much to observe.

I invite you, reader and internet user, to also make your observations.

Prof. Hartmut Glaser
CGI.br Executive Secretary

We at the Center for Technology and Society at Fundação Getulio Vargas Law School in Rio de Janeiro (CTS-FGV) are proud to present the "Internet Policy Report - Brazil 2011". This report analyzes some of the most relevant legislative and regulatory proposals affecting the Internet in Brazil during the year of 2011 and it is the first of its kind in the country. It is the result of a partnership between the CTS-FGV and the Brazilian Internet Steering Committee (CGI.br), through the project that became known as the Brazilian Observatory on Digital Policies, or simply the Observatory of the Internet.

The CTS-FGV was created nine years ago with the mission of conducting interdisciplinary research about the Internet and digital technology, producing knowledge to help develop the institutional, economic, social and cultural environment of the Internet in Brazil. Throughout these years the CTS-FGV has been collaborating with many individuals and organizations in the process of producing analysis on and discussing some of the main issues related to Internet regulation in Brazil, a role which has positioned the Center as one of the main Brazilian think tanks in the area. In this role the CTS-FGV has been acting as an advisor to the Brazilian government in organizing public consultations on bills to regulate the Internet such as the Regulatory Framework for the Internet and the Bill on Privacy and Data Protection.

This report reflects the work of many researchers who dedicated their time to write about such a interesting and instigating moment for Internet policy in Brazil. But more than that, it reflects a deeply democratic process of discussion which has involved countless participants, be them universities, companies, activists and individuals who care so much about their freedom on web. It tells the story of the regulation of the internet in Brazil during one of its most active years, a story which will be told again during many more years, and one which we are excited to share with you.

Bruno Magrani, Carlos Affonso and Ronaldo Lemos
Center for Technology and Society of the
Law School of the Getúlio Vargas Foundation

1

Internet Crimes: Bill no. 84/99

An adequate starting point for the assessment of Internet regulation in Brazil is Bill no. 84 from 1999.[1] It was proposed by representative Luiz Piauhylino to deal with Internet crime. The project, which also became known as "Lei Azeredo" ("Azeredo Bill")[2], was a turning point in Internet regulation in Brazil, as it fostered unprecedented social mobilization on Internet issues in the country.

It is noteworthy that this Bill was by no means the first or the only to foresee typification of Internet crimes. Over the last decades, several Bills have been proposed to regulate Internet conduct, several of which foresaw setting forth criminal criteria. PL 84/99 itself was, in fact, a result of the redesign and creation of a modified version of a former Bill proposed in 1996. What set this Bill apart from the rest – and led to the social mobilization that surrounded it – was that it "over" criminalized actions viewed as routine or trivial, or even indispensable to network innovation, followed by its quick transaction through approval instances under the slogan of preventing pedophilia and child pornography.

In addition to defining new Internet crimes, the Bill also set forth surveillance requirements and over extended the power of investigation of police forces,

---

[1] Available at: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>. Accessed on 03.05.12. In this chapter we'll use the terms "PL 84/99", "PL" and "Azeredo Bill" to refer to Bill no. 84, from 1999.

[2] The term "Azeredo Bill" refers to its main supporter, federal representative Eduardo Azeredo from the PSDB party of Minas Gerais.

which prompted some of the activists to refer to it as "Digital AI-5"[3], referring to a Decree during the military dictatorship that withdrew constitutional guarantees. The Bill 84/99 required Internet service providers and connection providers, for example, to retain user connection logs and access records for three years (article 22, I). Furthermore, it also required providers to notify police authorities confidentially whenever they suspected of criminal practices (art. 22, III). Also, its technically poor legislative writing defined unauthorized access to a computerized system as criminal – i.e. this in itself would criminalize reverse engineering, which is key to learning and technological innovation processes (art. 285-A).

Overall, although practices such as pedophilia, virus attacks and other revolting practices in the worldwide computer web must be coerced, there were scope and accuracy issues related to the content of the PL 84/99, which could lead to serious side effects.

A study by the Center for Technology and Society of the Law School of the Getulio Vargas Foundation detected several issues related to the Bill, which we present briefly below.[4] In regards to scope, the Bill's intention to only criminalize serious conducts was not attained to. Its devices, not only typified criminal conduct, but also created surveillance requirements for access and content providers, as well as requirements to provide data without the need for a court order. These requirements jeopardize fundamental rights of users, such as the right to privacy and due legal proceedings.

Furthermore, the technical inaccuracy of its content in regards to issues such as data protection is further proof of its threat to fundamental rights. The scope of criminal types foreseen by the Bill also encompasses trivial and routine actions

---

[3] Paulo Rená quotes an interview in which Sergio Amadeu describes how the term Digital AI-5 was coined: "Two youngsters came to interview me for the IG and the one who was filming said "hey, but this is like a digital AI-5". It was the anniversary of the AI-5 [it was 40 years since the Institutional Act no. 5 in December, 2008] and I was saying that when you make an exception into a rule and everyone is guilty until proven innocent, what you have is a State based on exceptions. When you say you have to capture and keep record of everybody's data, what you're saying is that everybody is a suspect. And this will create obstacles for telecenters, digital inclusion programs... If you go to a cafe in a city where there is an open network and the network manager is to be responsible for its use. No one will want to setup a network." SANTARÉM, Paulo Rená. O Direito Achado na Rede. p.81. Available at: <http://bit.ly/dissertacaoprenass>. Accessed on 18.07.12.

[4] LEMOS, Ronaldo et al. *Comments and Suggestions on the replacement for the Bill on Electronic Crimes* (PL no. 84/99), presented by the Committee for Constitution, Justice and Citizenship. Available at: <http://bibliotecadigital.fgv.br/dspace/handle/10438/7719>. Accessed on 16.07.12.

of users of the worldwide computer web, which could potentially criminalize the conducts of many users, which are usually regarded as legal or simply as torts due to being potentially less offensive.

Arguments against the PL 84/99 indicate that, in the current context of national legislation and the content of the Bill, its approval could considerably jeopardize comprehensive development of the Internet in Brazil. These risks both inhibits an innovative environment, where entrepreneurs can count on legal predictability and clear, pre-established civil rules, and could represent a threat to ensuring fundamental rights of users.

In order to foster innovation, a country must set forth precise rules to limit the liability of stakeholders; this ensures the safety and predictability of initiatives on the Web (such as investments, file maintenance, data bases, etc.). Criminal liabilities may only be set forth where civil rules fall short, at the risk of increasing the cost of investments and discouraging private, public and corporate initiatives in the industry. Special care must be taken to ensure that the criminal legislation designed is not excessively broad or vague, which is the case of the aforementioned bill. Lack of clear definition of criminal terms leads to uncertainty, particularly in regards to regulating such a complex topic that requires previous technical definition still pending in the country's legislative arena. Hence, legislators must be careful when regulating these issues. Accuracy must be ensured to fulfill legal purposes, but it must not overstep legal boundaries or be based on excessively broad concepts. Furthermore, any regulatory measure authorizing online activities monitoring, including storing user information, must also have limitations and counterweights to prevent abuse – which is not contemplated by the aforementioned Bill.

This perception has been broadly demonstrated by several agents involved in the debate on Internet regulation in the country, who refuted the Bill, PL 84/99, as well as by analyzes of international cases, which clearly demonstrate that the natural path of network regulation, followed by all developed countries, is to begin by setting forth a regulatory framework. This must set forth clear rules and responsibilities for users, companies and other institutions in regards to access to the network; this then shall be the basis for criminal regulations. Criminal law must be viewed as the last ratio, i.e. the last resort when all other regulatory measures fail.

One of the main arguments of those for the approval of the PL 84/99 was the alleged need to harmonize the Brazilian legislation with the Budapest

Convention. This Convention, also referred to as the Cybercrime Convention, was created within the jurisdiction of the European Council to set forth standards to fight online crime. It was approved on November 23, 2001 and Brazil was not involved. It came into effect only in 2004, after only 5 countries had sanctioned it. Although it allows adherence by any country in the world, to this date the text has only been ratified by a further 25 countries, particularly in Eastern and Central Europe. The text has never been sanctioned by Brazil, even after it was analyzed by several instances of the government (including the Ministry of Justice, the president's Institutional Security Office, the Federal Police Department, the Ministry of Science and technology and the Ministry of Foreign Relations), which assessed the alignment between the proposed content and the national structure. Hence, the content of the Convention must not be used as reference to support the country's legislation. The countries that committed to this Convention are mostly countries which have already implemented civil Internet regulation and, only after doing so, set forth criminal parameters for the Web. If we attempt to harmonize our legislation with the Convention, which hasn't even been approved by the Brazilian government, we'll risk going in the opposite direction – i.e. beginning by setting forth criminal sentences, before technical and civil regulation of the Internet in the country.

In regards to personal data protection, an assessment by Danilo Doneda has shown that the poor relationship between the registry and sensitive data set forth in the Bill – in regards to Police Authorities obtaining registry data from access and content providers – creates two issues:[5]

1. "The writer of the replacement used this category (sensitive data), which must be preserved and remain aside to enable specific protection in delicate circumstances (and, therefore, "sensitive"), excessively loosely, including each and every personal non-registry data. Hence, there is no differentiation between different types of sensitive data, which are leveled with all other personal data (and this consequently prevents in many offense situations the enforcement of basic individual rights). Hence, the Bill cannot be harmonized with international personal data protection trends;

[5] DONEDA, Danilo. *Novo texto do PL sobre crimes cibernéticos embaralha conceitos de proteção de dados*. Available at: <http://observatoriodainternet.br/novo-texto-do-pl-sobre-crimes-ciberneticos>. Accessed on 20.07.12.

2. The second issue is deeply-rooted: providing data protection guarantees only for sensitive data is a recurring idea on debates about the subject in Brazil. In addition to being impossible to reconcile with related fundamental rights -e.g. international standards for the industry -, this also jeopardizes the other guarantees related to personal data protection."

This situation jeopardizes basic individual liberties, and the implementation of an Internet surveillance system has prompted a lot of criticism from society against the Bill, which resulted in intense social mobilization.[6] Hence, despite the PL 84/99 being potentially harmful, the reaction against it brought together civil society, academia, industry and others.

One of the most evident examples of social engagement in connection with the Bill is the online petition entitled "Em Defesa da Liberdade e do Progresso do Conhecimento na Internet Brasileira" (For Knowledge Freedom and Progress in the Brazilian Internet)[7], which collected more than 160 thousand signatures requesting rejection of the Bill by the Federal Senate. Another example of popular engagement was the MegaNão[8] movement, which promoted several mobilization initiatives against the PL 84/99 inside and outside the Internet.

Hence, the reaction against the Internet crimes Bill fostered a network of digital activism and popular engagement in the Brazilian Internet Regulation process. This not only prevented its approval by the Congress, but also fostered key legislative initiatives to ensure freedom in the network and protection of user rights. Over the following chapters, we'll focus on the two main legislative proposals that stemmed from this movement: Internet Regulatory Framework[9] and the Personal Data Protection Act.

---

[6] An excellent account of the social mobilization prompted by the PL 84/99 is available in SANTARÉM, Paulo Renã da Silva. *O Direito Achado na Rede*: A Emergência do Acesso à Internet como Direito Fundamental no Brasil. Available at: <http://www.scribd.com/doc/41537075/Dissertacao-O-Direito-Achado-na-Rede>. Accessed on 12.07.12.

[7] Available at: <http://www.petitiononline.com/veto2008/petition.html>. Accessed on 01.06.12.

[8] Available at: <http://meganao.wordpress.com/>. Accessed on 01.07.12. The Mega Não! movement's involvement in opposing the PL 84/99 was awarded with the Frida award by the Internet Governance Forum. More information available at: <http://premiofrida.org/eng/>. Accessed on 12.07.12.

[9] Bill 2126 from 2011. Available at: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Accessed on 10.07.12.

Among the most recent developments of the project, the two public hearings held in 2011 are of note. The first[10] of these, carried out in July, was promoted by the Science and Technology, the Communication and IT, the Human Rights and Minorities, and the Public Safety and Fight Against Organized Crime committees. During this hearing, representatives of the Mega Não! movement handed the aforementioned petition to the representative Eduardo Azeredo. The hearing was broadcast on the Web and followed on Twitter on hashtags #cibercrimes, #AI5Digital and #MegaNão.

The second hearing[11], held in November, was attended by guests from several sectors of civil society and the academia to debate alternatives to the text of the Bill and the attached Bills.

On November 2011, as part of a political strategy to prevent approval of the PL 84/99, representative Paulo Teixeira, from the Labor Party of Sao Paulo, together with other representatives, proposed the Bill PL 2,793/2011[12], which also discusses typification of criminal IT infractions, but according to the suggestions of the Center for Technology and Society of the FGV Direito Rio.[13] The strategy consisted in approving a Bill that would contain at least the minimum requirements to coerce serious acts on the Internet, thus leaving the remainder of the network's regulation to the Internet Regulatory Framework. Hence, the new Bill substantially restricted the creation of new crimes and restricted typification of such crimes, attaining exclusively to absolutely indispensable conducts – as opposed to trivial, every day behaviors, which was the case of PL 84/99. It also eliminated the topic of user records retention (which was left to be dealt with by the Internet Regulatory Framework) and reduced the punishment for each crime. Representative Paulo Teixeira, as well as other representatives, namely Luiza Erundina (PSB-SP), Manuela D´Ávila (PCdoB-RS) and João Arruda (PMDB-PR), who wrote the Bill 2,793/2011, openly support the Internet Regulatory Framework.

---

[10] Available at: <http://www2.camara.gov.br/agencia/noticias/CIENCIA-E-TECNOLOGIA/199848-AUDIENCIA-DISCUTE-PROJETO-SOBRE-CRIMES-NA-INTERNET;-PARTICIPE.html>. Accessed on 03.03.12.

[11] Some videos of this hearing may be viewed at: <http://blip.tv/everton137/debate-sobre-crimes-praticados-por-meio-da-internet-no-brasil-incompleto-1472007>. Accessed on 01.07.12.

[12] Available at: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>. Accessed on 01.07.12.

[13] Available at: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/7719/coment%C3%A1rios%20ao%20substitutivo%20PL%2088-99.pdf?sequence=1>. Accessed on 01.07.12.

2

Internet Regulatory Framework

The Internet Regulatory Framework[14] is the main initiative for Internet regulation under assessment by the Brazilian National Congress. It resulted directly from the social movement that emerged with the Bill 84/99 and may be traced back to one of the main arguments used to prevent the advancement of the Bill. The main objective of the latter was to create criminal regulations manage the Internet – i.e. there was a need for prior civil regulation that would enable enforcing the rights and freedoms of citizens.[15] For this purpose, the president at the time, Mr. Luiz Inácio Lula da Silva, responding to the civil society's demands, launched during the X International Forum on Free Software (FISL), in 2009, an initiative aimed at proposing a "Regulatory Framework for the Brazilian Internet".[16]

In this context, inspired by Principles of Internet Governance and Use published by the Brazilian Internet Steering Committee[17], with massive popular support and

[14] Bill 2,126 from 2011. Available at: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Accessed on 12.07.12.

[15] LEMOS, Ronaldo. *Internet Brasileira Precisa de Marco Regulatório Civil*. Available at: <http://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm>. Accessed on 15.07.12.

[16] Available at: <http://congressoemfoco.uol.com.br/noticia.asp?cod_canal=1&cod_publicacao=30724>. Accessed on 21.05.12. In this publication we will refer to this proposal to regulate the Internet in Brazil as the Internet Regulatory Framework, or just Regulatory Framework. The version of the Bill used for the analysis presented herein is the one presented to the National Congress by the Federal Government, which is available at: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Accessed on 01.06.12.

[17] Brazilian Internet Steering Committee Resolution 2009-003. Available at: <http://www.cgi.br/regulamentacao/resolucao2009-003.htm>. Accessed on 17.07.12.

based on the government's guidelines, the Ministry of Justice's Department of Legislative Affairs (SAL-MJ), in partnership with the Getulio Vargas Foundation's Center for Technology and Society of the Law School of Rio de Janeiro (CTS-FGV), launched online an open and collaborative process to debate a Draft Bill setting forth basic laws for the Brazilian Internet. Following extensive debate involving several segments of society, the Draft Bill was finalized and presented to the National Congress. At the close of 2011, this draft was undergoing assessment by the House of Representatives as suit number 2,126 from 2011.[18]

In this item we will analyze the two main aspects of this regulation proposed: (a) the procedure, which focuses on innovation enabled by involving the population, through the Web, in the process of consultation, debating and writing the Regulatory Framework; and (b) the content, which deals with the man topics discussed in the Preliminary draft, such as Internet providers' responsibilities, website registration guard, among other relevant topics to the digital environment and its users.

2.1 A matter of process

A proposed Draft Bill to regulate the Internet could only be designed on the network itself. In this direction, one of the main innovations promoted by the Regulatory Framework was precisely its decentralized and open process of discussions with society, by using the tools available on the Internet itself. By adapting a blog creation platform known as WordPress[19] a system could be implemented to receive suggestions and comments through the Cultura Digital[20] website.

The public enquiry process was divided into two stages. The first stage began in October 2009 and lasted just over 45 days; a document containing general principles for the regulation of the network was posted for comments. These principles had been largely inspired by a resolution published by the Brazilian

[18] Bill 5403/01, Internet usage principles — House of Representatives Portal. Available at: <http://www2.camara.gov.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/54a-legislatura/pl-2126-11-principios-do-uso-da-internet>. Accessed on 27.07.12.

[19] Available at: <http://wordpress.com/>. Accessed on 18.06.12.

[20] Available at: <http://culturadigital.br/marcocivil/>. Accessed on 21.05.12.

Internet Steering Committee that listed "Principles for Governance and Use of the Internet in Brazil", also known as the CGI.br Decalogue.[21] Participants could then to elaborate on these principles and propose new topics to be covered by future legislation.

During this initial stage, in excess of 800 comments were received, systematized and used as reference for the preliminary draft submitted to public enquiry in an online platform, initially available for 45 days. Due public demand, this second step was extended for another week and ended on May 30, 2010.

In the last stage, there were approximately 1,200 comments on the document. As well as individuals and civil society organizations, domestic and foreign companies related to the culture and technology industries were also involved, which promoted increased diversity of opinions and, therefore, legitimized the process.

A partial balance carried out halfway through the second stage revealed that, up to that point, the most popular discussion topics had been related to proposing a voluntary mechanism that would exempt Internet service providers from any liabilities for third-party content. This exemption, however, would be conditioned to the voluntary adoption of a response mechanism for extrajudicial notifications – both from the party who allegedly incurred damages and the publisher claiming title and wishing to guarantee the availability of the content published. However, several claims pointed out the difficulties of implementing a mechanism of such nature, in particular the potential risks to constitutional rights, such as freedom of speech.

Thus, as evidence that the debate was indeed open and collaborative; a new text was prepared from the various contributions received. Internet service providers' liability for content posted by third parties was conditioned to the receipt and breach of a specific court order; that is, a court order would be required for providers and the likes to be obliged to remove third party content, such as comments on blogs, tweets, forum entries or videos posted by users.

Besides comments on the online platform, the public debate on the Regulatory Framework also benefited from the intense activity in other network channels, such as comments on blogs and on Twitter. Searching for the hashtag # marcocivil, during the consultation period, provided a good thermometer of the massive

[21] Available at: <http://www.cgi.br/regulamentacao/resolucao2009-003.htm>. Accessed on 13.06.12.

engagement. Several entities, companies and organizations, as well as individuals, sent their contributions via the process' contact e-mail address. These documents, most of which were extensive, analyzed the entire draft under consultation, and were made available to the public and also open for discussions in the online platform. This measure increased transparency and openness of the debate.

Actual face-to-face discussions, organized by the SAL-MJ staff or independently, as well as public hearings held throughout the two stages across the country, had a fundamental role. These meetings promoted debates and were essential for raising awareness of the Regulatory Framework.

At the end of the public debate, the team working on the Regulatory Framework, which included SAL-MJ and CTS/FGV representatives, was responsible for compiling all comments, determining prevailing viewpoints, making due changes and, finally, presenting society with the final document to be sent to the Brazilian Congress.

The Regulatory Framework revolutionized the democratic nature of the legislative process. By enabling virtually anyone to participate in the debate on a future bill, the initiative parted with the concept of public hearings as the main occasions for interested parties to have a say on the legislative process. Rather than rendering these hearings obsolete, the online platform actually complemented the whole experience in-person debates in public hearings. Furthermore, the process involving public hearings and discussions in the corridors and offices of representatives in Brasilia is biased towards companies and interest groups that have the means to attend these in-person meetings. The process carried out through the Internet, in turn, helps resetting the balance of this equation by enabling otherwise under represented segments of society to engage more.

Furthermore, it is worth noting that the document will inevitably undergo changes when submitted to the Brazilian Congress and discussed in legislative houses. Far from being a distortion of the nature of the initiative, the fact that the Congress has received a document based on months of discussions online, changes the role of legislators to that of perfecting something that was not created by a single office alone, but by the collective intelligence of an entire community.

Thus, legislators who wish to propose changes to the Regulatory Framework are faced with a challenge and a realization: the challenge of improving the product of many and the realization that the changes they make will not go unnoticed, because the resulting text of the Regulatory Framework will certainly be broadly

disclosed on the Web and discussed in various forums and social networks. The high transparency of the debate on the Regulatory Framework naturally creates revision marks on any future legislative work.

There is also a matter of principle in the process of producing the Regulatory Framework. This principle stems from the belief that the best regulatory framework shall be the one initiated through the network itself and based on the enforcement fundamental rights. Therefore, the Regulatory Framework is intrinsically principled. it aims to set forth guidelines, parameters and objectives that will be further detailed and developed by legislators, governors, judges, as well as students and researchers of topics related to Web development.

2.2 Topics addressed by the Regulatory Framework

The contents of the Regulatory Framework may be divided into six parts: (i) fundamentals, principles and objectives; (ii) user rights and guarantees; (iii) providers' liabilities; (iv) record retention by Internet providers; (v) network neutrality; (vi) the role of the Government. We'll briefly analyze each of them below.

2.2.1 Fundamentals, Principles and Objectives

The Regulatory Framework, as a highly principled law and in line with the general structure of the Constitution, initially sets forth the fundamentals, principles and objectives for the topic of the Internet in Brazil. These three dimensions are the pillars that will support the interpretation and enforcement of the Regulatory Framework, of future Internet legislations, as well as – and perhaps more importantly – future situations for which there are no specific legal provisions.

The first pillar comprises fundamentals of the Internet. These are: acknowledging the worldwide scale of the network, human rights and the potential to exercise one's rights as citizen through digital media, plurality and diversity, openness and collaboration, free enterprise, free competition and consumer protection.

The second pillar is comprised by general principles for the Internet, which include: enforcement of the constitutional right to freedom of expression, communication and to speak one's mind, privacy protection, personal data protection, preserving and ensuring network neutrality, preservation of stability, security and network functionality, by implementing measures consistent with

international standards and by encouraging the use of best practices; agents' accountability based on their activities, according to the legislation, and, finally, preservation of the participatory nature of the network.

The next topic of the Regulatory Framework sets forth the objectives that must be taken into account when regulating the Internet, knowingly: promoting the right of all citizens to access the Internet; promoting access to information, knowledge and engagement in cultural affairs and management of public affairs, promoting innovating and fostering sharing of new use and access technologies and models; promoting adherence to open technology standards that enable communication, accessibility and interoperability between applications and databases.

2.2.2 User Rights and Guarantees

In addition to these general principles underlying interpretations of the Regulatory Framework, there is a separate chapter in the bill on user rights and guarantees. While the first ensure alignment with the values set forth in the Federal Constitution, the latter stresses these values by ensuring freedom of expression and privacy in communications.

In article 7 of bill PL 2,126/11, access to the Internet is described as essential for exercising one's rights as citizen, which guarantees that Internet communications must be inviolable and confidential, as well as that connections and the quality contracted must be uninterrupted, as per the subsections of this article.

Ensuring uninterrupted Internet connection services, except due to default, is a measure that aims to prevent ultra restrictive models against copyright infringement, such as the HADOPI law (*Haut Autorité pour La Diffusion des Oeuvres et laProtection des droits sur Internet*) in France, from being implemented in Brazil. The French model by which copyright breaches are punishable by blocking connection, known as "progressive response" or "Three Strikes Law", is a bill proposed as an attempt to curb illegal downloading of songs and videos published through *peer-to-peer*[22] networks. The law foresees that three warnings must be issued before punishing the transgressor by discontinuing his/her access to the Internet.

[22] For more information on *peer-to-peer* technology, check out: <http://en.wikipedia.org/wiki/Peer-to-peer>. Accessed on 12.06.12.

The first step following notice of a suspected breach of copyrights to the administrative body of the HADOPI is to notify the user that he/she is potentially in breach of copyrights. If the referred content is not removed, the user will be formally notified by the organization and, if he/she insists, his/her connection will be suspended for the duration of the investigation by the Public Prosecutor. If the breach is confirmed, the user may be legally prevented from contracting any access provider for up to one year, in addition to being fined and potentially having to continue to pay for the provider's services, despite having his/her connection cancelled.[23,24]

The Regulatory Framework intends, therefore, to show the importance of having access to the Internet and to prevent it from being arbitrarily discontinued, which sets it apart from the French initiative that foresees otherwise. It is worth noting again that the aforementioned disposition of the Regulatory Framework makes an exception only for service discontinuation due to payment default.

2.2.3 Internet Providers' Liabilities

One of the core aspects of the Regulatory Framework involves regulating providers' responsibilities. The importance of regulating this topic is directly related to two values it aims to protect, knowingly: ensuring freedom on the network and fostering innovation. We will analyze how providers' responsibilities affect each of these two topics, but first we must understand why Internet providers are naturally targeted by governments on issues related to information and investigations on the network.

Providers are the "middle men" in communications between Internet users. As such, they enjoy a privileged position that confers them great power (albeit not necessarily rightfully so) over what traffics on their networks. Hence, techniques such as data package inspections or filtering enable providers to restrict, monitor or block Internet communication for certain data, addressees and senders.

---

[23] Available at: <http://legifrance.gouv.fr/affichCodeArticle.do;jsessionid=44FCC56BE74A4FAB1E45C368440683DB.tpdjo16v_3?cidTexte=LEGITEXT000006069414&idArticle=LEGIARTI000021212151&dateTexte=20120518&categorieLien=id#LEGIARTI000021212151>. Accessed on 01.06.12.

[24] Available at: <http://legifrance.gouv.fr/affichCodeArticle.do;jsessionid=44FCC56BE74A4FAB1E45C368440683DB.tpdjo16v_3?cidTexte=LEGITEXT000006069414&idArticle=LEGIARTI000021212156&dateTexte=20120518&categorieLien=id#LEGIARTI000021212156>. Accessed on 01.06.12.

Some authors have been referring to these providers as online gatekeepers[25], that is, agents who have the actual power to interfere (by aiding or hindering) on traffic through their networks. The Regulatory Framework foresees a functional distinction between different Internet providers, by splitting them into applications providers (online services) and connection (or access) providers – these categories relate the responsibilities to the roles actually played by each type.

Providers are also key to identifying users on the network. Both services and applications providers and access providers are needed to locate a user on the Internet. Hence, when, for example, a piece of information is posted on a social network – which, according to the Regulatory Framework, is an applications provider – the user leaves a record of his/her IP address. This address is the first step towards identifying the end user.

The second step requires identifying which user was using that IP address at the exact time when the information was posted. This, in turn, can only be achieved through the Internet connection provider, which keeps subscriber access records. Nevertheless, these data will enable finding a device (computer/client) and will not necessarily identify the individual who actually posted the information. It may not be possible to identify the user when he/she has used a proxy or any other anonymization technology, when the user connected through third party computers or when access took place at a public place. If, on one hand, there are several obstacles to locating a user, on the other hand, the service providers that host unlawful information are easily located; hence why they attract so much attention from parties who may have suffered damages. This is why several lawsuits in the Brazilian Judiciary have been relying on the so-called third party accountability.

Making third-parties accountable is a recurrent resource in several other areas of the Brazilian legal system. The Civil Code, for example, sets forth that in certain cases when third parties are accountable for actions which they did not cause[26],

---

[25] ZITTRAIN, Jonathan. *A History of Online Gatekeeping*. Harvard Journal of Law and Technology, Vol. 19, No. 2, p. 253, 2006. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=905862>. Accessed on 12.06.12.

[26] Law 10,406/2002 (Civil Code):
"Article 932. The following are also liable for civil remedy:
I - parents, on behalf of their underage children who are under their care and in their company;
II - tutors and curators on behalf of their pupils and protégés who find themselves in the same conditions;
III - employers or principals on behalf of their employees, workers and representatives in the course of the work assigned to them or in connection with it;

such as: parents are accountable for the actions of their underage children under their care or in their company, tutors or curators are accountable on behalf of their pupils or protégés, or even employers may be accountable on behalf of their employees. In such cases, the rationale behind making them accountable is based on a duty of care, vigilance or custody between the parties that, when breached, generates responsibility for negligence or recklessness.

The Civil Code also sets forth a modality of liability in which the third party is accountable even if there is no party at fault, provided that "the activity commonly practiced by the perpetrator of the damage, by its nature, poses risks to others".[27] Likewise, the Consumer Protection Code sets forth that service or product providers are accountable for potential damages caused by their products or services[28], irrespective of being at fault or not (which is referred to in the doctrine as "objective liability").

Although there are several cases in the Brazilian legal system that foresee third-party accountability, applying these to Internet providers may be extremely detrimental to the development of the network. Excessive accountability by applications or service providers for the damages caused by their users pushes these providers towards monitoring and censoring any data that could potentially lead to a lawsuit or governmental sanctions.

Furthermore, this liability model would virtually turn private companies into censorship agents with powers to monitor, judge and implement pre-censorship on individuals, with no option to appeal or any control over abuses. Hence, ensuring that Internet providers have limited liabilities is, in fact, guaranteeing that the users of their services are effectively free to express

---

IV - owners of hotels, inns, houses or facilities that provide lodging in exchange for money, even if for educational purposes, on behalf of their guests, moderators and students;

V - those who freely take a share of the products of a crime, up to the relevant amount."

[27] Law 10,406/2002 (Civil Code):
"Article 927. He/she who, by carrying out illicit act (articles 186 and 187), causes damage to someone else, is hereby obliged to repair it.
Single paragraph. There will be an obligation to repair the damage, regardless of fault, in cases specified by law, or when the nature of the activity normally undertaken by the perpetrator poses risk to the rights of others."

[28] Law 8,078/1990 (Consumer Protection Code):
"Article 12. Domestic or foreign manufacturers, producers, builders and importers are liable, regardless of fault, for repairing damages caused to consumers by defects resulting from design, manufacture, construction, assembly, formulation, handling, presentation or packaging of their products, as well as insufficient or inadequate information about their use and risks."

themselves and communicate through the network. It is worth noting that this does not imply that occasional damages do not have to be repaired, only that the individual who actually caused the damage shall be liable, not the "middle-man" in the process.

Another important value that providers' liabilities limitations aim to preserve is innovation on the network. It is intrinsic to the innovation process that the tools and applications created will have unexpected consequences. This is particularly true when the intended collaborative and open nature of the Brazilian Internet is taken into account, since making such technology available to the general public means that the uses that will follow are even more unpredictable.

Hence, in order to prompt application providers to produce innovative technologies, with not always predictable effects, we must ensure a certain degree of limitation to their liabilities, particularly regarding third-party use of the technology. Pamela Samuelson, from the Berkeley University, has shown the importance of limiting the liabilities of the "middle-men" who develop technology by analyzing the Sony vs. Universal[29] case, which created an essential precedent to protect the enormous wave of innovation in the information technology industry in the U.S. in the 80s.

In this important case, ruled by the U.S. Supreme Court, Sony was found innocent and not accountable for the videos recorded by users enabled by Sony's home VCR (Sony Betamax). Limiting business risks is critical for innovation. While well established companies can afford the costs of the odd lawsuit, new technology enterprises (i.e. startups) are not as financially sound and are particularly susceptible to legal demands. In economic terms, limiting providers' liabilities significantly reduces barriers to entering the market and promotes competition, which are values protected by the Brazilian Federal Constitution.

Perhaps the most prominent international paradigms on Internet providers' liabilities are the Digital Millennium Copyright Act (DMCA)[30] – a section of the U.S. copyrights law that specifically addresses Internet and digital technologies

[29] SAMUELSON, Pamela. *The Generativity of Sony v. Universal: The Intellectual Property Legacy of Justice Stevens*. Fordham Law Review. Vol. 74, p. 1831, 2006. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=925127>. Accessed on 30.06.12.

[30] Code of Laws of the United States of America, section 17, paragraph 512.

– and the Communications Decency Act (CDA)[31] – North American act that regulates defamation of indecent materials on the Internet.

The DMCA has created an ample system to manage intellectual property in digital technologies. Generally, this section sets forth guarantees for providers against liabilities due to copyrights breaches by third parties, conditional to providers complying with certain obligations related to handling and removing content.

While access providers (Transitory Digital Network Communications)[32] are usually exempt from any liabilities, provided that data transfer through their networks is automated, online service providers are subject to liabilities when they fail to takedown infringing content, when requests by copyrights holders.[33] This model is known in international doctrine as "notice and takedown", for it sets forth an extrajudicial system in which copyrights holders may notify application or service providers to remove copyrights protected works from their websites.[34]

This system has been criticized for the chilling effects of the abuse of the right to send takedown notifications on providers and users.[35] Since service providers' liability is established when they fail to execute a takedown notice, there is a clear incentive for providers to execute all notices, without necessarily analyzing their source.

The CDA, in turn, differs from the DMCA in both its object and approach to liability and incentives to stakeholders. In regards to its object, while the DMCA applies to intellectual works, i.e. works protected by copyrights, the object of the CDA is defamatory and fake information that expose minors and others to explicit content. Contents of defamatory nature are the most closely related to the hypotheses covered by the Regulatory Framework. Furthermore, the CDA sets forth that Internet services providers are not to be construed as publishers, which exempts the first from the usual legal liabilities for contents published.

---

[31] Code of Laws of the United States of America, section 47, paragraph 230.

[32] Code of Laws of the United States of America, section 17, paragraph 512, item (a).

[33] Code of Laws of the United States of America, section 17, paragraph 512, item (d).

[34] For more information on provider liability systems in the U.S. legislation see ZITTRAIN, *op. cit*.

[35] On this topic, see the Chilling Effects Clearinghouse project created to assess the legitimacy of takedown notices sent by copyrights holders. Available at: <http://www.chillingeffects.org/>. Accessed on 12.06.12.

The first case that supports the argument that service providers should not be construed as publishers and, consequentially, could not be held liable for contents published by third parties is the *Cubby, Inc. vs. CompuServe, Inc*[36] case. The court argued that as service providers they were not screening materials before these were posted by third parties, hence they could not be held liable. This case was later reversed by the trial of the *Stratton Oakmont, Inc vs. Prodigy Services Co.* case. However, the CDA reinstated the premise of the *CompuServe* case and took it a step further. In addition to exempting providers from liabilities for third party content, the CDA further exempted them from other liabilities were they to take the necessary measures, in good faith, to take down defamatory or damaging content, etc.[37] This CDA model is known as the good Samaritan model, because it prompts providers to voluntarily remove content that could be damaging, thus preventing any liabilities for its potential damages.

Looking into the international experiences and the intense debates and suggestions made during several public consultations, the Regulatory Framework has chosen a model that sets it apart from the North American notice and takedown system, in that it grants more robust exemption of liabilities to applications providers for contents created by users of their services. While in the U.S. providers may still be subject to abuse by excessive use of notices by online copyrights holders, the Regulatory Framework ensures that providers will only be held liable for third party content if they fail to execute a court order. Hence, the original version of the bill presented to the National Congress stated:

> *Article 14. Internet connection providers shall not be held liable for damages caused by third party content.*
>
> *Article 15. Except as otherwise provided by law, Internet applications providers shall only be held liable for damages caused by third party content if they fail to*

[36] Case 776 F. Supp. 135 of the US District Court for the Southern District of New York, 1991.

[37] The definitions of the CDA include other cases that constitute variations of obscene or indecent conducts. The actual text states:

"47 U.S.C. § 230

(c) (2) *Civil Liability*

No provider or user of an interactive computer service shall be held liable on account of–

(A) *any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected*; (...)".

> *execute a specific court order, within the scope of their services and the term set forth, to take down content deemed infringing.*
>
> *Single paragraph. The court order referred to in the header above, subject to becoming void, must clearly specify the content deemed infringing to enable the referred material to be unequivocally located.*
>
> *Article 16. Whenever in possession of contact details for the user directly responsible for the content referred to in article 15, the Internet applications provider must notify the user of the execution of the court order.*

It is noteworthy that the Regulatory Framework has adopted a functional distinction between connection and applications providers to set different liabilities for each of them. *A priori* they are both not liable for third party content; however, while connection providers have absolute immunity, which cannot be revoked, applications providers are only exempt from liabilities if they execute all court orders to take down content.

Some critics of the bill argued that, although providers were protected, there were no guarantees for citizens against private censorship practices carried out by providers as a result of potential agreements made. However, this argument does not seem to hold for two reasons – i.e. a market-related and a legal reason.

First of all, providers of applications that allow third parties to publish content, in view of the nature of this activity, are set to benefit from promoting more publications; hence, it will not be in their best interest to censor them. If users realize that a specific provider allows a wide range of uncensored publications, this will add value to the provider's services because users will migrate to it and competition will promote more freedom.

Second of all, when market dynamics does not ensure freedom (such as when network effects prevail, or when censorship pressures outweigh freedom pressures), there are specific institutions in the Brazilian legal system that set forth limitations to providers' rights to censor content.

Hence, unjustified access restrictions and abusive censorship measures in general that might result from potential agreements, may be deemed as direct abuse, which is restrained by Article 187 of the Civil Code[38] The nature

[38] Law 10,406/2002 (Civil Code).
Article 187. "Holders of rights who, by exercising their rights, clearly exceed the limits imposed by their economic or social purpose, by good faith or by good moral conduct shall be also in breach of the law."

of their activity and their limited liability puts providers in a position in which they can negotiate to prevent such agreements. Nevertheless, if such agreements are made, market incentives combined with legal limitations will ensure that these respect the rights of users, subject to sanctions provided for in the legislation.

A further criticism related to the previous one is that, in practice, users would have their freedom of expression restricted, because only a small number of users would resort to lawsuits against abuses by providers due to the inaccessibility of the legal system. In response to this argument, in addition to the aforementioned incentives to prevent providers from censoring, the final section of the Regulatory Framework allows for rights to be protected by a collective. In other words, associations, trade associations, the public prosecutor's office and other institutions may file lawsuits against providers who abuse their prerogative to take down content. This is expected to prompt widespread supervision of the acts of providers and, at the same time, to address the issue of asymmetrical access to the Legal System.

Furthermore, it is worth noting that, albeit not ideal to promote freedom of expression, the proposal above does not seem to promote otherwise. By promoting otherwise we mean creating a system in which applications providers who receive third party content are obliged to allow publication of any information, except when requested otherwise by a specific court order. This restriction would probably be deemed unconstitutional as it is strongly opposed by the principle of freedom of enterprise, set forth in articles 1 (subsection IV) and 170 of the Federal Constitution.

Let's picture a situation in which an entrepreneur decides to create a private forum to discuss episodes of the known sitcom Game of Thrones. Since there already are several similar forums online, we'll say that what would set this one apart would be the fact that it would enable users to discuss each episode in a separate topic. Hence, users would not have to worry about finding information on future episodes that could spoil the surprises of the series. In order to do that, the forum would have moderators who would exclude all inappropriate comments that could defeat the purpose of the website. A system that obliges providers to publish all contents would render this model, and several other business models that involve moderation from providers, unfeasible. Such system would excessively restrain the scope of private enterprise and should be avoided.

Finally, it is also worth noting that the bill for the Regulatory Framework sent to the Congress foresees it as a general standard applicable to any content on the Internet, regardless of whether it is protected or not by copyrights. If a copyrights act is instated in the future, it will supersede the Regulatory Framework, but, until then, the latter will be the general rule. It is noticeable that the current proposal being debated to regulate the liabilities of Internet providers, under the scope of the review of the copyrights legislation, foresees a very similar model to the North American DMCA.

2.2.4 Record Retention by Internet Providers

User records retention by Internet providers is one of the most controversial topics of the Regulatory Framework. The fact that this topic is addressed by the bill can only be understood by looking into the context that led to it.

The Regulatory Framework, as seen in this chapter, was created as reaction to bill 84/99, which aimed to define a range of Internet crimes. One of the dispositions of this bill set forth that providers had to keep records of connection and access to Internet applications for three years, which led to this topic being included in the Regulatory Framework to prevent advancement of the criminal debate. In incorporating the topic of record retention, the draft was carefully crafted to restrict cases when access to such records would be permitted, as well as how long they should be kept for.

In article 5, VI, the Regulatory Framework defines connection record as a set of information on the start date and time of a specific connection to the Internet, as well as its duration and the IP addresses used by the terminals sending and receiving data packages. A *record of access to applications*, in turn, is defined as a set of information on the use date and time of a specific Internet application from a particular IP address. The Regulatory Framework foresees that connection records and access records may only be disclosed to the police with a specific warrant and for specific purposes, clearly stating that such restrictions are key to protecting the privacy, honor and image of people.

Furthermore, in its disposition about paid or free *connection* it forbids retention of records on access to Internet applications. On the other hand, in its disposition on Internet *applications* it allows access records retention. Nevertheless, the text foresees the possibility of requiring disclosure of records of access to Internet applications, provided that a court order is issued and that such records are

relative to specific facts and to a specific period of time, ensuring users' constitutional rights.

The requirement of a court order to obtain information that enable identifying a user or to oblige applications providers to keep access records prevents the police and the Public Prosecution from requesting such data, irrespective of court orders. Nevertheless, the bill foresees the possibility of authorities requiring providers to keep certain records, but a specific court order is still required for data disclosure.

The Regulatory Framework also sets forth a period of one year for connection records retention. The aim of this disposition was to find a balance between the need to keep records to enable police investigations and the need to protect citizens' privacy. The one year term for record retention is in line with recent statistics of use of user data requested by investigative authorities in European countries.[39]

According to a recent report[40], approximately 56% of all data from Internet user records used in police investigations had been retained for three months or less, 19% were up to six months old and 18% had been kept for up to 12 months. In order words, 93% of all data requested for police investigations had been retained for up to 1 year, which indicates that the term set by the Regulatory Framework seems sufficient to cover police demand. Restricting records retention for as little time as possible is key to protecting people's privacy.

2.2.5 Network Neutrality

For a thorough debate on neutrality regulation on the network please see item 3 of this report.

2.2.6 The Role of the Government

The final chapter of the Regulatory Framework discusses the role that the Government is expected to play, aiming to steer the actions of all federative bodies regarding the development of the Internet in Brazil.

---

[39] Report From The Commission To The Council And The European Parliament Evaluation report on the Data Retention Directive (Directive 2006/24/EC). Available at: <http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf>. Accessed on 03.03.12.

[40] Idem.

For that, the need for transparent, democratic and collaborative governance principles is highlighted, as well as the need to promote technological interoperability between the federal bodies that provide electronic government services. The document advises these bodies to favor open and free technologies, standards and formats. This section of the Regulatory Framework may, however, find resistance in the future in view of an injunction by the Supreme Court from 2004, which revoked a law from the state of Rio Grande do Sul that set forth preferential rights for purchasing open code software.[41]

Furthermore, the document also fosters public initiatives focused on promoting digital culture and the Internet as a social tool. The aim of this provision is to promote digital inclusion, to reduce inequalities between different regions of the Country in regards to access to and use of information and communication technologies, and to foster domestic content production and circulation.

[41] Injunction granted by ADI no. 3059, ruled by the Brazilian Supreme Court.

3

Network Neutrality Regulation

The concept of network neutrality is best understood as a network design principle, according to which all information carried through the network must be equally treated. Tim Wu explains that "the idea is that a maximally useful public network aspires to treat all content, sites and platforms equally. This allows the network to carry every type of information and support every kind of application. The principle suggests that information networks are often more valuable when they are less specialized – when they are a platform for multiple uses, present and future. (For people who know more about network design, what is just described is similar to the "end-to-end" design principle).[42]

In other words, the principle establishes that Internet access providers[43] should not block the use or limit the traffic speed of specific applications or content in their networks. Likewise, the idea that access providers (the operators offering Internet access services to end customers, such as NET Virtua, Oi, Telefonica, GVT, etc.) should

[42] Tim Wu's definition of network neutrality as seen at: <http://timwu.org/network_neutrality.html>. Accessed on 06.03.12.

[43] The terms "Internet access providers", "Internet providers" or "access providers" will be used to identify telecommunications enterprises offering Internet access services. Although the Internet's distributed nature primarily implies that everyone located at its endpoints is an Internet user, the term "user" in this publication will be restricted to consumers of Internet services, whether private individuals or businesses, whose main activity does not involve providing online content or services. On the other hand – and subject to relevant exceptions – the term "content providers" shall refer to enterprises or private individuals that provide online content and services to the public as their main activity. Once again, the differentiation does not aim to be exact or foolproof; on the contrary, its objective is to give the reader a general idea.

charge service or content providers (the platforms that offer online services, such as search engines, social networks, blogging and video platforms, etc.) different fees for its users to have faster or privileged access to a particular content or application, could also be considered contrary to the network neutrality principle. Those who champion the principle claim it to be the main guarantee that the Internet will continue being a free and unrestricted platform for innovation.[44] Furthermore, it ensures that barriers to market entry will continue limited, allowing individuals and small enterprises to innovate and compete with established businesses.

The network neutrality debate is not new. It has concerned scholars since the beginning of the 2000s, within the broader concept of end to end design.[45] In Brazil, network neutrality violations have been reported at least since 2004. One of the first cases involved the operator Brasil Telecom, which blocked voice over IP calls.[46] In 2006, Velox, the Internet service of the operator Oi, started discriminating against specific content on the pretext of guaranteeing its users' safety.[47]

At a first glance, it would seem that Internet access providers have no reason to discriminate against particular data packets in their networks. Common sense would expect that the more applications and content provided, the more attractive the service to users, generating a competitive edge over data restricting providers. However, over the years, providers have shown that there are incentives to discriminate against or block applications or content, and that these are strong enough to promote such actions.[48]

Based on concrete cases occurring in the US, Professor Barbara Van Schewick, from Stanford University, identifies three groups of situations in which Internet providers are encouraged to discriminate against data packets on the Web. Firstly, providers can discriminate to increase profits at the expense of users. Thus, there is a clear incentive to, for instance, take action against applications that compete with other services offered by the provider, as in the case of restrictions to voice

---

[44] VAN SCHEWICK, Barbara. *Internet Architecture and Innovation*. Cambridge: MIT Press, 2010.

[45] In this respect see LESSIG, Lawrence and LEMLEY, Mark A. *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=247737>. Accessed on 03.01.12.

[46] See AFFONSO, Carlos A. *Todos os datagramas são iguais perante a Rede!.* PoliTICs magazine.

[47] Note that these incidents were prior to the Oi-Brasil Telecom merger.

[48] VAN SCHEWICK, Barbara and FABER, D. Point/Counterpoint: Network Neutrality Nuances. *Communications of the ACM*. New York, v. 52, n. 2, p. 32, 2009.

over IP services (when the provider offers its own telephone services), or even limit the use of programs based on the bittorrent protocol (when providers offer video on demand services). This category would also include the proposal to change Internet providers' business model, allowing them to charge content providers to share their data with users more quickly. This would not replace the fee already paid by users to access the Web, but would rather create an additional source of income for providers. Whether or not providers should be allowed to freely implement such practices is a source of great controversy. Generally speaking, on the one hand it is argued that the additional revenue would be invested in infrastructure, either to increase network capacity and speed or to reduce access costs for users.[49] On the other hand, critics of this practice allege that a) there is no guarantee that the additional profit will be reinvested in infrastructure or used to reduce prices; b) it does not promote social well-being, as it limits users' choices; c) it further impedes the entry of new competitors in the market, thus restricting innovation.

Providers also have incentives to discriminate against packets for traffic management in their networks. As most providers charge end customers a fixed monthly rate for their services, while acquiring Internet access from other providers based on their volume of data traffic, any increase in Internet traffic raises their expenses without generating extra income. Therefore, they are encouraged to hinder the traffic of applications and content that consume excessive bandwidth, such as clients who use bittorrent or websites offering video streaming. Traffic management can thus serve as a pain killer with immediate effects, but which does not solve the bigger problem of network congestion. Traffic management capability is essential for the operation of any network. During peak user times, poor management can render certain applications useless. Therefore, for example, if an e-mail takes two minutes to be delivered, rather than a few seconds, this will not cause significant damages or render the tool useless, but a 1- or 2-second response delay in a voice over IP will seriously jeopardize the service. This does not mean that users should be able to have unlimited bandwidth capacity, but that the user, and not the provider, should decide how best to use the contracted bandwidth.

---

[49] For all, see YOO, C. S. Innovations in the Internet's Architecture that Challenge the Status Quo. *Journal on Telecommunications and High Technology Law*. Available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1472074>. Accessed on 06.03.12.

Finally, Internet access providers also have an incentive to block content that goes against their interests and does not conform to their content policy, or content which might generate liability.

Several of the issues that the network neutrality principle attempts to prevent would not occur in a competitive market. If a service does not respect a user's choice and imposes limitations to his/her access, the solution would be to simply change provider. As long as users value the possibility of accessing content and applications of their own choice, a competitive market will naturally offer such service.

Historically, the telecommunications market has been regarded as a natural monopoly.[50] However, studies dating from the end of the 20th century showed that the telephone monopoly in the U.S. was less due to natural market features and more a result of reiterated government action.[51] Nonetheless, a study carried out by the National Telecommunications Agency and presented during the public enquiry on the General Plan for Competition Targets (PGMC) concluded that, in the Brazilian infrastructure and broadband market, a single company controls a significant share of the market by over 3,758 cities.

Despite this analysis, there is great controversy as to whether a competitive Internet access market would suffice to preserve the Internet's characteristics that the network neutrality principle seeks to safeguard.[52] Van Schewick believes regulation is necessary even under these circumstances. Based on the end to end principle, which views the Internet as a multipurpose application-agnostic tool, she identifies three main traits which allowed the Internet to become the great innovation platform of the last decades: a) innovators on the Web have always enjoyed freedom to create applications; likewise, users have always enjoyed freedom to independently choose which applications to use; b) the application-blindness of the network ensured that providers could not interfere with these choices, i.e. that they could not distort competition among applications or reduce application developers' profits through access charges; c) finally, the low costs of innovation on the Internet not only fostered the

[50] SPULBER, D.F. Deregulating Telecommunications. *Yale Journal of Regulation* 12(1), (1995): p. 25-67.

[51] Idem.

[52] In this respect, see VAN SCHEWICK, B. op. cit., YOO, C.S., op. cit., WU, T. Network Neutrality, Broadband Discrimination. *Journal of Telecommunications and High Technology Law*, v. 2, p. 141, 2003. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863>. Accessed on 15.12.11.

development of more applications, but also allowed a large and diverse group of people to become innovators, which in turn increased the overall amount and quality of innovation.[53]

Based on this analysis, Van Schewick establishes criteria to evaluate non-discrimination rules, which we believe are extremely useful to the process of drafting a network neutrality rule. These are as follows:

c) "...by protecting the factors that have fostered **application innovation** in the past, we can make sure that the Internet will be even more useful and valuable in the future;

d) It should protect the factors that allowed the Internet to foster **democratic debate** and provide a decentralized environment for social and cultural interaction in which anyone can participate;

e) It **must not affect the development of the network** anymore than necessary to reach network neutrality regulation goals;

f) It should **simplify** the task of **determining what kind of behavior** is or not allowed, to reassure industry stakeholders;

g) It must keep **regulation costs low**."

3.1 Neutrality Regulation in the International Scenario

In recent years, governments and regulation agencies worldwide, responding to increasingly frequent examples of network neutrality violation, initiated a process of discussing and implementing the first rules on network neutrality. Following the lead of Chile, which approved in 2001 the world's first network neutrality law, Colombia also adopted a standard in its national development plan to curb information discrimination practices. In the European Union, Holland pioneered the implementation of a specific regulation.

---

[53] VAN SCHEWICK, B. Opening Statement at the Federal Communications Commission's Workshop on Innovation, Investment and the Open Internet in Cambridge, MA on January 13, 2010, WC Docket No. 07-52, GN Docket No. 09-191. Available at: <http://cyberlaw.stanford.edu/publications/opening-statement-federal-communications-commission%E2%80%99s-workshop-innovation-investment>. Accessed on 05.03.12.

In the US, the Federal Communications Commission (FCC) has debated and experimented with rules to guarantee network neutrality since 2005.[54] Following several public consultations, media debates and closed-door meetings with industry representatives, the commission finally issued regulations aimed at guaranteeing network neutrality in the country, which were then enacted in November 2011.[55] The basic FCC rules on network neutrality are as follows:

a) **Transparency**. Fixed and mobile broadband providers must disclose network management practices, performance features and the terms and conditions of their broadband services;

b) **No blocking**. Fixed broadband providers must not block lawful content, lawful applications and services, or devices that do not hinder network performance; mobile broadband providers must not block lawful websites or applications that compete with their voice or video telephony services; and

c) **No unreasonable discrimination**. Fixed broadband providers must not unreasonably discriminate against lawful network traffic.

For those who defend the network neutrality principle, the rules are yet timid. Firstly, their application to mobile broadband services is limited to merely prohibiting blocking of services that compete with the providers' specific services. Secondly, there is still a margin for discrimination, as long as it is deemed "reasonable." The vague definition of what would be considered unreasonable discrimination may lead to abuse, which will demand FCC time and resources for close monitoring.

It is interesting to note that the proposal to regulate network neutrality in the US was strongly influenced by Latin American proposals and legislation on the topic. For purposes of illustration, we have included below a chart mapping out the presence of the main elements of the FCC's neutrality rules in several Latin American legislations.

---

[54] US Federal Communications Commission. Policy Statement FCC 05-151. Available at: <http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260435A1.pdf>. Accessed on 13.07.12.

[55] US Federal Communications Commission. FCC Resolution 10-201. Available at: <http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf>. Accessed on 18.07.12.

COMPARATIVE CHART OF THE FCC'S OPEN INTERNET BASIC FREEDOMS WITH LEGISLATION AND LEGISLATIVE PROPOSALS FROM CHILE, ARGENTINA, COLOMBIA, BRAZIL, MEXICO AND VENEZUELA

FCC's Basic Freedoms for Network Neutrality	Chile	Argentina	Colombia	Brazil	Mexico	Venezuela
Freedom of access to any lawful content	Article 24, H, a)	Bill 1159-D-2011 Article 1, a) Bill S-1491/11 Article 1	Law 1,450 from 2011, Article 56, 1.	Draft Bill – Internet Regulatory Framework Article 10, header. Anatel Regulation, Article 59, header.	Bill to amend the Federal Telecommunications Law Article 44	None.[56]
Freedom to run any lawful application	Article 24, H, a)	Bill 1159-D-2011 Article 1, a) Bill S-1491/11 Article 1	Law 1,450 from 2011, Article 56, 1.	Draft Bill – Internet Regulatory Framework Article 10, header. Anatel Regulation, Article 59, header.	Bill to amend the Federal Telecommunications Law Article 44	None.

[56] See footnote 57.

COMPARATIVE CHART OF OTHER KEY ISSUES IN LEGISLATION AND LEGISLATIVE PROPOSALS FROM CHILE, ARGENTINA, COLOMBIA, BRAZIL, MEXICO AND VENEZUELA (CONTINUATION)

FCC's Basic Freedoms for Network Neutrality	Chile	Argentina	Colombia	Brazil	Mexico	Venezuela
Freedom to connect any devices that do not affect network operation (carterfone)	Article 24, H, b)	Bill 1159-D-2011 Article 1, b)	Law 1,450 from 2011, Article 56, 2.	Not included in specific neutrality regulations.[57] Not included in specific neutrality regulations.	Not included in specific neutrality regulations.	None.
Access to comprehensive information on service plans (transparency)	Article 24, H, d)	Bill S-1491/11 Article 2	Law 1,450 from 2011, Article 5,6, 4.	Draft Bill – Internet Regulatory Framework Article 8, IV. Anatel Regulation, Article 59, paragraph 2	Not included in specific neutrality regulations.	None.

[57] Non-inclusion in the specific neutrality regulation does not mean the freedom is not foreseen by other regulations.

COMPARATIVE CHART OF OTHER KEY ISSUES IN LEGISLATION AND LEGISLATIVE PROPOSALS FROM CHILE, ARGENTINA, COLOMBIA, BRAZIL, MEXICO AND VENEZUELA (CONTINUATION)

	Chile	Argentina	Colombia	Brazil	Mexico	Venezuela
Are there exceptions to the neutrality principle for technical or safety reasons?	Yes. Art. 24, H, a)	Bill 1159-D-2011 Yes. Article 1, c Bill S-1491/11 Yes. Article 3.	No, it wouldn't.	Yes. Article 10, header. Yes. Article 59, paragraph 2.	No, it wouldn't.	Not applicable.
Are providers obliged to offer parental guidance services upon users' request?	Yes. Art. 24, H, a)	Bill 1159-D-2011 Yes. Article 1, c.[58] Bill S-1491/11 No, it wouldn't.	Yes. Article 56, 3.	No, it wouldn't. No, it wouldn't.	No, it wouldn't.	Not applicable.

[58] The article provides for the possibility of users requesting providers to block content of their choice, which can be interpreted as allowing, among others, parental control by providers.

3.2 Proposals for Network Neutrality Regulation in Brazil

In line with the global regulatory movement, two proposals to regulate the network neutrality principle emerged in Brazil in 2011: article 10 of the Internet Regulatory Framework[59] and article 59 of the Multimedia Communications Providers Quality Regulation[60], open for public comments by the National Telecommunications Agency (Anatel).

The Internet Regulatory Framework proposal submitted to the National Congress in 2011, analyzed in the second chapter of this publication, set forth the following rules for the network neutrality principle:

> *Article 10. Those responsible for transmitting, commuting or routing are obliged to treat all data packets with* ***isonomy****, making no distinctions based on content, origin and destination, service, terminal or application, and* ***any traffic discrimination or degradation not directly related to technical requirements in connection with the services provided is forbidden****, according to regulation by the National Telecommunications Agency – Anatel on the preservation and guarantee of network neutrality.*

The header of article 10 sets forth a general prohibition of differential treatment of Internet data packets by providers. This prohibition covers both discrimination and degradation practices. The reason for including both practices is to ban not only occasional blocks, but also network management practices which prioritize specific applications or content to the detriment of others. It also bans the charging of different rates by providers, based on the type of application or content accessed by users. This aims at preventing providers from distorting competition on the Web by increasing barriers to new competitors. The established rule is commensurate with the previously mentioned end to end principle and aims at guaranteeing the preservation of the principles listed by Van Schewick.

---

[59] Bill no 2,126 from 2011 under assessment by the House of Representatives. Available at: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Accessed on 18.07.12.

[60] Annex to Public Consultation no. 45 of the National Telecommunications Agency. Available at: <http://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C1514&Tipo=1&Opcao=>. Accessed on 18.07.12.

One must acknowledge, however, that it is impossible to implement the neutrality principle in full, and that it is essential to guarantee some degree of traffic management autonomy, due to certain technical requirements. An absolute rule would forbid, for example, any attempt to prevent the transmission of spam or deter denial of service (DoS)[61] attacks, since the countermeasures needed to stop such attacks require blocking access originated from certain computers. Given the need to create exceptions to the general neutrality rule, the Internet Regulatory Framework gives Anatel the power to regulate such cases.

There are other ways in which the neutrality principle can be made flexible. For instance, the option adopted by the US Federal Communications Commission was to forbid unreasonable discrimination in transmitting network traffic. The problem with this regulation is the lack of objective criteria to help define what should be considered lawful exceptions. To be effectively implemented, it would depend exclusively on the judiciary, which, without the necessary technical knowledge and lacking other criteria on which to base its decisions, might interpret the norm in a totally different way from its original purpose.

Besides delegating regulation to a technically competent agency, the legislative proposal could have adopted additional criteria to help the agency establish which practices would constitute exceptions to the neutrality principle.

The single paragraph of article 10 expands on the aim of establishing neutrality to ban practices involving network traffic monitoring, filtering, analyzing or inspecting.

> *Single paragraph. When providing paid or free Internet access, monitoring, filtering, analyzing or inspecting data packet content is forbidden, subject to exceptions foreseen by the legislation.*

Besides reinforcing the prohibition of network content blocking, there was an additional concern with preventing a practice known as deep packet inspection, which consists of analyzing packet content carried through the Web by intermediaries that should only transport them.[62] This practice came under

---

[61] For a simplified explanation of denial of service attack see: <http://pt.wikipedia.org/wiki/Ataque_de_nega%C3%A7%C3%A3o_de_servi%C3%A7o>. Accessed on 01.07.12.

[62] For an overview of the technology, see: <http://en.wikipedia.org/wiki/Deep_packet_inspection>. Accessed on 20.07.12.

criticism when an American company started closing deals with Internet access providers to monitor which sites its users accessed and offer them targeted advertising based on their browsing history.[63] This does not imply, however, a total ban on Internet data monitoring and the exception provided for at the end of the paragraph could be applied to the hypothesis foreseen in paragraphs 2 and 3 of article 13 of the Internet Regulatory Framework.[64]

The other initiative aimed at regulating the network neutrality principle in Brazil is found in public consultation no. 45 promoted by Anatel, which addressed the issue as follows:

> *Article 59. Providers are forbidden to engage in blocking or discriminatory treatment of any kind of traffic, such as voice, data or video, regardless of the technology used.*
>
> *1. The prohibition provided for in the header of this article does not prevent implementation of blocking or traffic management measures that are* ***paramount for security and service stability****, as well as, the stability of the networks that support them;*
>
> *2. The blocking and traffic management criteria set forth in paragraph 2 of this article must be previously informed to all subscribers and broadly disclosed to all interested parts, including publishing in the providers' websites;*
>
> *3. Blocking and traffic management measures must respect the privacy of subscribers, the confidentiality of communications and free, universal and fair competition.*

Despite the similarity between the Anatel and the Internet Regulatory Framework proposals concerning a general prohibition of discrimination, the former has some advantages over the latter. First of all, it outlines in greater detail which exceptions to the neutrality principle are allowed (i.e., only those related to

---

[63] For a summary of the monitoring practices developed by the company Phorm, see: <http://en.wikipedia.org/wiki/Phorm>. Accessed on 20 July 2012.

[64] Bill 2,126 from 2011. Article 13. When providing Internet applications providers may keep users' access records at their discretion, subject to the provisions of article 7.
[...]
2. A court order may determine record keeping for a certain period of accesses to Internet applications, provided the records relate to specific facts in a definite period, and that information disclosure is subject to the provision of Section IV of this Chapter.
3. Subject to the provisions of paragraph 2, police or administrative authorities may apply for custody of the Internet application records, according to the procedures and terms of paragraphs 3 and 4 of article 11. 11.

security assurance and **service stability**). This specification restricts the exceptions and reinforces the general principle. Moreover, the rule establishes a more rigorous requirement for potential exceptions than the Internet Regulatory Framework. While the framework's regulation prohibits "traffic discrimination or degradation not directly related to technical **requirements** of the services provided," the agency's proposal adopts the criterion of **indispensability**, and its hypotheses are more restricted.

Furthermore, Anatel's regulation calls for obligatory transparency in the eventuality of discriminatory practices, which is essential for consumers to adequately compare services offered by different Internet providers and make informed decisions.

Finally, it is worth noting that while the general rule of the Internet Regulatory Framework would apply to any kind of access to the Internet, Anatel's regulation would only cover multimedia communications services businesses, that is, Internet providers. Internet access via mobile phones would not be constrained by the regulation's neutrality rule.

Despite these criticisms, the proposals are an important step in safeguarding network neutrality and preserving the Internet's original technical characteristics.

4

Privacy

Twenty-eleven was a significant year for the debates on privacy and data protection in the digital environment. In Brazil, there were two noteworthy regulatory proposals: a Bill called **Internet Regulatory Framework** and the Draft Bill on Personal Data Protection, which were both open to public debate through a procedure inspired by the **Regulatory Framework**. Moreover, the Act on Access to Information retained by public organizations and non-profit private entities, which have received public funds, was approved. This act is key as it positions the Internet strategically for the enforcement of the constitutional right to access to information.

4.1 Privacy and personal data

The development of information technologies, of the Internet in particular, has yielded undeniable benefits to society, such as convenient and fast communications. On the other hand, scientific progress has also fostered new ways to invade the privacy of others. In addition to that, the Internet itself is an inviting environment for privacy violation, since most users are unaware of how their personal data is collected and used when they browse the network.

In view of the context briefly described above, the concept of privacy and its protection could not help but evolve. Moving away from the concept of "being left alone", which is an individualist concept that aims to restrict State intervention into people's lives, the current concept of privacy is related to the

need for more control over the use of personal data. Hence, the right to privacy takes on the important role of protecting personal data, by enabling control over several means of handling such information (i.e. collection, retention and use). This control not only safeguards data owners, but also the society to which these individuals belong, since such data could reveal sensitive information (e.g. race, political, religious and sexual preferences, etc.) of discriminatory potential.

Brazil foresees legal protection to privacy in article 5, subsections X, on intimacy and private life, and XII, which guarantees the inviolability of correspondence, home and communications. The Constitution, on subsection LXXII of the same article, grants individuals the right to access information concerning them and retained in governmental or public records or databases, as well as the right to amend such data. This is the constitutional remedy of *habeas data*, instated by law 9,507, from November 12, 1997. The Civil Code also addresses the issue of privacy setting forth the inviolability of private life, in the chapter on entity's rights (article 21).

Unlike other countries, including our neighbors Argentina and Uruguay, Brazil still lack a general law on personal data protection. A Draft Bill on the topic was submitted to public debate in 2011, as described later in this document. The only regulation that specifically addresses personal data protection, in addition to the law that legitimates seeking *habeas data*, is the Consumer Protection Code – i.e. articles 43 and 44 of the latter regulate retention of databases and consumer registries, foreseeing a series of consumer guarantees.[65]

4.2 Regulatory initiatives and proposals affecting how privacy is handled in Brazil

4.2.1 Draft Bill on personal data

In 2011, the public debate on a proposal for a normative framework for privacy and personal data protection was concluded. The Draft Bill resulted from a partnership between the Ministry of Justice and the Brazilian Observatory

[65] It is also worth noting the Complementary Law 105, from January 10, 2001, on the confidentiality of financial operations, which sets forth a few rules that affect personal data protection, in article 1 of paragraph 3.

of Digital Policies, and its primary objective was to ensure that citizens held control and title over their own personal information, which would uphold the constitutional right to privacy. The debate began on November 30, 2010 and was prolonged until April 30, 2011.

The Draft Bill is of relevance to digital policies from the perspective of at least three aspects, which will be discussed below.

4.2.1.1 Data leakage

One of the main challenges (and concerns) created by being able to easily register large volumes of information is the risk of them "leaking" or being unduly disclosed. In regards to personal data, its use is even more frequent and necessary for activities carried out by the public and private sectors. Lack of a management policy for such information leads to careless and excessive treatment, thus increasing the risk of accidental or even intentional public disclosure.

Cases of data leakage have become common, including in Brazil, and learning about these, understandably, causes citizens and consumers to become suspicious of the organizations that allowed such disclosures. Also, even when the data does not actually reach public domain, data leakage can cause actual damages in several circumstances. Furthermore, this poses a technical and organizational challenge for the corporations handling such data. Hence why it has been the object of increasing and intensive regulation abroad, as we'll see below.

The Draft Bill on personal data also addresses the issue by setting forth that such data must be handled so as to reduce the risk of unauthorized access to a minimum (article 23). Hence, the one who processes the information must implement technical and administrative measures proportional to the current state of technology, the nature of the data and the specific characteristics of its processing, so as to prevent, among other damages, accidental or unlawful disclosure or unauthorized access to personal information (physical and logical security principle – article 8, subsection VII). Furthermore, these measures, whenever possible, must prevent such damages (prevention principle – subsection X, article 8).

Processing personal data is deemed a risky activity by the Draft Bill. This means that in the event of leakage of personal data or any other damages to property or moral, individual or collective damages, the one directly processing the data shall be liable (article 6).

4.2.1.2 Sensitive data processing

Another controversial and worrying topic is sensitive data processing, which are personal data whose nature may lead to discrimination against their owners. The Draft Bill lists ethnic or racial information, religious, philosophical or moral convictions, political opinions, union memberships, parties and religious affiliations and philosophical or political affiliations as examples of sensitive data, as well as, health, genetic and biometric data, and data related to the sexual conduct of individuals (article 4, subsection IV).

The importance of sensitive data to certain activities carried out in the digital environment is clear and, in some cases, it is the very nature of the activity. This is the case of social networks, which rely on constantly processing personal data, many of which are sensitive, and their input by service users themselves.

The Draft Bill dedicates a chapter to regulating sensitive data processing. It starts of by forbidding compulsory disclosure of such data (article 21) and forbids creating databases that reveal, directly or indirectly, data of such nature, except when otherwise permitted by express legal disposition. The Draft Bill, however, lists a few situations in which sensitive data processing is allowed, such as with the holder's consent and when it is essential for compliance with legal or statutory attributions by its user (paragraph 1, subsection I), for research purposes (subsection IV) or if the data has been made public by its title holder (subsection V). In turn, use of sensitive data to discriminate against its holder is illegal (paragraph 2, article 21).

4.2.1.3 Behavioral advertising

Behavioral advertisement is another activity that involves processing personal data online and may have negative repercussions on consumer privacy protection. This type of advertisement which involves, for example, placing ads on users' e-mail pages based on their habits and interests may be useful, but also extremely inconvenient for those on the receiving end. Furthermore, this practice may be viewed as an invasion of privacy as it is based on gathering information from personal correspondence, i.e. the person's e-mail account.

In regards to this topic, the Draft Bill foresees that personal data may only be processed with the holder's prior consent and such consent must be free, express and informed (article 9). Furthermore, as per one of the fundamental principles of the Draft Bill, data may only be processed for the purposes that originally led

to their collection and of which the holder is aware. Processing is attached to the "specific, explicit and legitimate" purposes of the one responsible for data use (article 8, subsection I). Hence, behavioral advertisement is prohibited if it involves data processing for which the express consent of the data holder has not been obtained.

Use of sensitive data must also comply with the specific dispositions for this type of data referred to in the previous item.

4.2.2 Privacy in the Internet Regulatory Framework

Another noteworthy regulatory proposal for digital policies in the country is the Draft Bill entitled Internet Regulatory Framework. By setting forth principles, guarantees, rights and obligations for the use of the Internet in the country, the Regulatory Framework foresees privacy and personal data protection, which requires the used guarantee in the Internet services agreement to clearly state the personal data protection regimen, connection records and records of access to applications retained (article 7, subsection IV).

One of the issues directly related to the topic is addressed by the Draft Bill, namely disclosure and retention of connection records[66] and records of access[67] to Internet applications. Since these data could potentially reveal personal information, the Draft Bill requires these records to be retained and disclosed so as to preserve the intimacy, the private life, the honor and the image of the parties directly or indirectly involved (article 10).

In the general section on records retention, the Draft Bill sets forth that the provider responsible for retention shall be obliged to disclose information that will lead to identification of the user by court order (article 10, paragraph 1). If the confidentiality right foreseen by the Draft Bill is breached, the violator shall be liable to civil, criminal and administrative sanctions.

---

[66] Comprised by data on the start and end dates and times of a connection to the Internet, its duration and the IP address used by the terminal sending and receiving data packages (article 5, subsection VI).

[67] Set of information related to the date and time of use of a specific Internet application from a particular IP address (article 5, subsection VIII).

In regards to Internet connection records, the autonomous system administrator[68] is obliged to retain such records under strict confidentiality, in a controlled and safe environment for one year. The duration of record retention may be extended by cautionary requirement from a legal or administrative authority (article 11, header and paragraph 2). On the other hand, whether the connection is provided freely or paid for, connection providers are prohibited to retain access records (article 12). Such access records may be retained by the Internet applications provider or not, provided that user rights foreseen in article 7 are upheld. Retaining such records may be compulsory if required by court order, if these are related to specific facts over a specific period (article 12, paragraph 2).

4.2.3 Law on access to public information

Access to public information is currently viewed as one of the cornerstones of democracy. The premise is that a well informed citizen is better prepared not only to known his/her basic rights, such as health, education and social benefits, but also to effectively engage in the decision-making process of decisions that will affect him/her (CGU, 2011).

Several international organizations, including the United Nations and the Organization of American States, recognize access to information as a basic right. Along the same lines, approximately 90 countries currently have specific legislations on the topic.

In Brazil, law no. 12,527, from November, 18, 2011, governs the right to access to information, which had formerly been foreseen by the constitution (articles 5, subsection XXXIII; 37, subsection II, paragraph 3; 216, paragraph 2 of the Federal Constitution).

Law 12,527/2011 is based on the concept that the information produced, stored, organized and managed by the State on behalf of society is public property. Hence, there is a paradigm shift in terms of public transparency, as it sets forth that access should be the norm and secrecy the exception (CGU, 2011). Any citizen is, therefore, entitled to request such public information, provided that

[68] "Individual or enterprise that manages blocks of specific Internet Protocols (IP) addresses and their respective autonomous routing system, duly registered with the national authority in charge of IP address registration and distribution in the Country" (article 5, subsection III).

it hasn't been classed as confidential, following a set procedure that will be discussed later.

Public bodies and organizations from the three instances of Power (i.e. Executive, Legislative and Judiciary), from all levels of the government (federal, state, district and municipal), as well as the Audit Court and the General Attorney's Office, independent agencies, public foundations, public companies, the mixed-economy society and other entities controlled directly or indirectly by the Country, States, the Federal District and Municipalities (article 1). The law also applies to non-profit private organizations that have received public funds to carry out public interest activities (article 2).

This law is an important contribution to digital policies, since it foresees the potential of communication media, enabled by information technologies, to uphold the right to access to information (article 3, subsection III). Furthermore, it instates active transparency by obliging public bodies and organizations to disclose information of public or general interest produced or kept by them, through easy-access media, including websites (paragraph 2). The information to be disclosed includes addresses, phone numbers and opening hours of governmental units, general data on governmental programs, actions, projects and works, and answers to society's FAQs.

For citizens' requests to access information, the law sets forth specific terms by which data must be disclosed, knowingly the response must be immediate if available, or issued within 20 days extendable for additional 10 days. The request does not need to be justified, it only requires the applicant's identification and specification of the information required. The applicant may appeal if his/her request is denied or if access is refused (article 15).

There are, however, exceptions to this rule, such as personal data and other information deemed confidential by authorities.

Personal information are data related to "the individual identified or identifiable" (article 4, IV); the law foresees that these must be processed transparently and preserving the intimacy, private life, honor and image of people (article 31). These data require express consent from the holder or legal provision for disclosure or to be made accessible to third parties. However, there may be no need to obtain the holder's consent to access personal information in cases in which access to the information is required for the following: a) medical prevention and diagnosis, when the holder is physically or legally unfit, and

for medical treatment; b) statistics and scientific research of public or general interest, but disclosing the identity of the data holder is strictly forbidden; c) court order execution; d) human rights protection; and e) protecting public and general interest.

Other restricted information is deemed confidential information. The general rule is that public information may only be deemed confidential if essential to society's protection (i.e. to protect the population's life, security or health) or to protect the State (national sovereignty, international relations, intelligence activities).

Public information may be classified as: i) top secret, which must be kept confidential for 25 years, extendable for another term; ii) secret, which must be kept confidential for 15 years and iii) reserved, which must be kept confidential for 5 years (article 24).

The law sets forth which authorities are entitled to classify information, based on the different levels of secrecy. The stricter the confidentiality, the higher the rank of the public agent (article 27). However, access to information or documents on human rights violations by public agents or on behalf of public authorities cannot be restricted (article 21).

4.3 Regulatory initiatives and proposals affecting how privacy is handled internationally

4.3.1 Personal data protection laws

In 2011, a few countries approved regulations for personal data protection, which has evidently affected how such data is treated on the Internet. Peru has joined a group of Latin American countries, including Chile, Argentina, Uruguay, Mexico and Colombia, which has implemented specific legislation on the topic, based on the European regulatory experience. The so-called *Ley de Protección de Datos Personales* (*Ley No. 29733*) was proposed by the Presidency as a means of aligning Peru with its free commerce agreements with the United States and Canada, and with its future agreement with the EU.[69]

[69] Available at: <http://www.huntonprivacyblog.com/2011/08/articles/english-translation-of-perus-law-for-personal-data-protection-released/>.Accessed on 20.07.12.

In the Asian scenario, two key initiatives were implemented. In April, 2011, India adopted new rules on privacy, known as Information Technology Rules. These rules foresee a series of obligations for corporations handling personal data. Such obligations require corporations to set forth new privacy policies, to restrict sensitive data processing and international data transfer, as well as to implement additional security measures. The new rules are somewhat similar to the European legislation on privacy and its implementation is viewed as a challenge for service providers and consumers.[70]

China, like Brazil, does not have a seamless regulation on personal data protection. Nonetheless, in September, 2011, the Province of Jiangsu published its Information Technology Regulation, which includes provisions on personal data collection and use, as well as sanctions to breaches of such provisions. China has several regulations on personal data protection, but most of these are specific to certain areas (electronic commerce or banking). The Regulation is viewed as an important stepping stone towards creating national personal data protection legislation in the country.[71]

[70] Available at: <http://www.huntonprivacyblog.com/2011/05/articles/india-drafts-new-privacy-regulations/>. Accessed on 20.07.12.

[71] Available at: <http://www.huntonprivacyblog.com/2011/11/articles/new-chinese-legislation-includes-provisions-protecting-personal-information/>. Accessed on 20.07.12.

5

Internet regulation in the reform of the Copyrights Law: article 105-A of the proposal

Following a long process of hearings, seminars and meetings involving several sectors of society, which began in 2007, the Ministry of Culture, during the mandate of João Luiz Silva Ferreira ("Juca Ferreira"), prepared a Draft Bill for the reform of the Copyrights Law (LDA – Law no. 9,610, from 1998); this led to a period open for public comments in June, 2010.

Acknowledging how the current law is mismatched and all of the issues that follow, the Juca Ferreira administration, under president Lula's Government and in line with the former administration, by reviewing the law, intended to create an instrument to consolidate the economy of culture in the country. This law was also aimed at protecting the constitutional rights of authors and society to access education, information and culture. Historically, this is the first time that we take a progressive stance on copyrights regulation.

During the first period open for public comments, the Ministry of Culture presented very clear rationale and answers, which enabled society to understand the government's exact intentions for reviewing the law. The main objectives of the proposal include: increasing and ensuring effective support and protection to authors and their creations, balancing the rights of all stakeholders, increasing and democratizing access to cultural goods and services by the population, aligning the legislation with new paradigms created by the digital environment and enabling the State to create public

policies to foster, oversee, regulate and protect society's and the country's interests domestically and in international forums.[72]

In January 2011, Ana Buarque de Hollanda took over the Ministry of Culture and due this change in administration the Draft Bill to review the Copyrights Legislation was remitted back by the Presidential Staff to the Ministry of Culture. During the review of the draft by the minister of Culture and by the Board of Intellectual Rights of the Department of Cultural Policies, new changes were proposed and a decision was made to reopen for public comments.[73]

The process of opening for public comments took place between April 25 and May 30, 2011, but this was less democratic and less transparent than the former, only opening for expert comments and on particular topics. Following this preparatory stage of the Draft Bill, the document was submitted again to the President's Office, where it is currently under analysis for submission to the National Congress.

Among the changes made, there is a particular exert of interest in regards to Internet regulation. The document sent to the President's Office, on article 105-A, foresees solidary liability for content providers who fail to take the necessary measures to take down allegedly infringing content at the copyrights holder's request. Hence, the article sets forth that:

> *Article 105-A. Internet applications providers may be held solidarily liable, under the terms of article 105, for damages due to unauthorized public disclosure of works and phonograms by third parties, when they fail to take the necessary measures to take down allegedly infringing content, within the scope of their services and within reasonable time, following notification by the victimized copyrights holder or the publisher.*
>
> *§ 1 Internet applications providers must ostensibly provide at least one electronic channel through which notices and counter notices may be received, and may, at their discretion, provide an automated mechanism to handle the procedures foreseen in this Section.*
>
> *§ 2 The notifications referred to in this item must contain the following, subject to being voided:*

---

[72] See <http://www.cultura.gov.br/site/2010/04/12/nota-a-sociedade-sobre-a-revisao-da-lei-de-direito-autoral/>. Accessed on 15.05.10.

[73] The rules for the new period for public comments are on their website: <http://www.cultura.gov.br/site/2011/04/20/ultima-fase-da-revisao-da-lda/>. Accessed on 03.03.12.

I - identification of the notice's author, including full name, civil and tax registration numbers and updated contact details;

II - sending date and time;

III - clear and specific description of the allegedly infringing content, which must enable unequivocal identification of the material by the receiver;

IV - description of the relationship between the author of the notice and the allegedly infringing content; and

V - legal rationale for the removal.

§ 3 When content is taken down, it is Internet applications providers duty to notify the person who originally disclosed the content publicly, providing the reason for the removal and setting a reasonable term for permanent removal of the infringing content.

§ 4 If the person accountable for the content cannot be identified or located, and provided that all requirements to validate the notice have been complied with, Internet applications providers must ensure the content remains blocked.

§ 5 The person who originally disclosed the content publicly, provided that the requirements set forth in paragraph 2 are complied with, may submit a counter notice asking for the content to be made available again and accepting full liability for potential damages to third parties; in which case Internet applications providers shall be obliged to restore access to the content made unavailable and notify the author of the original notice.

§ 6 Any other individual or corporate stakeholder, provided that the requirements set forth in paragraph 2 are complied with, may counter notify Internet applications providers, accepting full liability for disclosure of the content.

§ 7 The authors of the original and the counter notices are legally liable for false or misleading information and for abuse or bad faith.

§ 8 Users who moderate third-party content, for the purpose of this article, have the same legal liabilities as Internet applications providers.

Firstly, we must stress that the proposal foresees taking down allegedly infringing content, before assessment of the validity of the request by the provider or a Legal Authority. In other words, the holder has the power to decide on the legality of using the work, which may cause a few problems. That is because the possibility that the provider may be held liable is incentive enough for providers to take down content without questioning upon receiving notices by copyrights holders. Holders, in turn, have sufficient incentives to notify any unauthorized use of their work.

While in some cases there will be no doubt about the infringing character of the use of a certain work, in many other cases there'll only be an individual

and contextualized assessment to determine illegal use. There may be cases, for example, in which the use may only limit copyrights, as foreseen in articles 46 onwards of the LDA, in which case there is no requirement for the author's consent. There may also be cases in which the works are already in the public domain, and prompting providers, users and holders may remove otherwise freely and legally available content from the Internet.[74] Hence, the provision as it is may lead to abuse of copyrights, thus significantly restricting certain rights, such as the right to freedom of expression and copyrights exceptions and limitations.

Although paragraph 5 of the legal provision allows – content publishers to choose to counter notify providers to maintain content availability -; it is very likely that publishers, albeit certain of the legality of their conduct, may choose not to counter notify providers to avoid becoming liable for the costs of expensive legal proceedings.[75]

By choosing to counter notify providers, users accept full liability for the content and potential damages caused, and Internet providers are obliged to immediately restore access to the content. Furthermore, according to paragraph 6, any other interested party may counter notify the provider, provided that this party accepts full liability for potential copyrights violations by the author of the original publication.[76]

Moreover, one of the objectives of article 105-A is to align the Copyrights Legislation with the scheme foreseen in the Internet Regulatory Framework. That is because, following extensive debates during the period in which the Internet Regulatory Framework was open for comments, a requirement for a court order to remove any allegedly infringing content was introduced. Hence,

---

[74] It is worth noting that this is not as remote a possibility as some might think. On the contrary, as demonstrated by Professor Sergio Branco, in his book "O Domínio Público no Direito Autoral Brasileiros" ("Public Domain in the Brazilian Copyrights Legislation"), there are already several cases of public archives that simply ignore public domain and restrict and charge for the use of public works.

[75] § 5 – The person who originally disclosed the content publicly, provided that the requirements set forth in paragraph 2 are complied with, may submit a counter notice asking for the content to be made available again and accepting full liability for potential damages to third parties; in which case Internet applications providers shall be obliged to restore access to the content made unavailable and notify the author of the original notice.

[76] § 6 – Any other individual or corporate stakeholder, provided that the requirements set forth in paragraph 2 are complied with, may counter notify Internet applications providers, accepting full liability for disclosure of the content.

alignment of these two proposals should move towards a requirement for a court order to remove allegedly infringing content in the current bill.

As debated in the context of the Internet Regulatory Framework, approving a system in which intermediates shall be liable for content published by third parties will create an economic incentive for the first to remove content, prior to any assessment by a Legal Authority on the illegality of the allegedly infringing information.

6

Internet Governance

6.1 Internet Governance in the International Scenario

Internet governance refers to the processes by which agreements, principles, rules of conduct, and decision-making related to the Internet emerge. The main objectives of the Internet system of governance are, on the one side, to ensure the network's smooth operation and, on the other, to share information and best practices so as to advance towards harmonized and compatible policies.

The system of Internet governance has some particular characteristics that distinguish it from most other international systems: 1) it is multi-sectorial – i.e. many stakeholders (such as governments, civil society, the private sector, and the technical and academic communities) participate in it with relative equality; 2) the legitimacy of the system's participants arises mainly from their expertise and ability to contribute to the process of policy design; 3) the results of governance processes do not always materialize in formal agreements or treaties; self-regulation, soft law[77] and good practices play an important role in advancing the system.

[77] A variety of instruments fall under the generic umbrella of soft law. This designation includes treaties with vague or weak obligations that establish general goals and action programs, as well as non-binding instruments, such as resolutions and terms of conduct. They are voluntary and may be designed collaboratively by governmental and non-governmental organizations. Chinkin, C. *The Challenge of soft law: development and change in international law*. International and Comparative Law Quarterly, vol 38. New York: Cambridge University Press, 1989, p. 851-2.

Internet governance may be applied to various levels – national, regional and global – that influence each other. The decisions made at the international level, for example, affect and restrict regulatory and policy options at the national level.

The issues discussed in international forums dedicated to Internet governance are closely related to network users' interests: they concern, among other issues, privacy, access to content, freedom of expression, security, and strategies for increasing access and reducing connection costs. Therefore, observing international discussions is of paramount importance to influencing future Internet regulatory policies.

6.2 Overview of Internet Governance in 2011

Throughout 2011, Internet governance became a highly politicized issue. Seemingly, the belief that Internet governance is a purely technical issue related to infrastructure and critical resources (domain names and IP numbers) management has been superseded. The politicization process of the issue is not new, but it has become accentuated, primarily by WikiLeaks' repercussions and the relevance of the Internet in social activism, as seen with the Arab Spring.

Examples confirming the issue's increasing importance on national political agendas abound: the seminars promoted by the Council of Europe, the conference in Vienna on the Internet and human rights, the forum on Internet freedom preceding the G8 summit at Deauville, and discussions within the IBSA (India, Brazil, and South Africa) Forum. Concomitantly, the issue has expanded beyond communications and technology ministries, which increases the challenges of coordinating Internet governance policies in the governmental sphere.

Issues related to cybersecurity and human rights took focus. Various incidents including information leaks, coordinated acts by hackers and crackers, and DDoS attacks prompted discussions on security in communication media. There were also efforts to put certain issues, such as online intellectual property protection, on the spotlight in security discussions, through an ongoing process of intensification of enforcement and increased penalties. At the same time, discussions on freedom of expression and association on the Internet and the potential negative implications of security policies on human rights, including on privacy, gained momentum.

In the international arena, a consolidated understanding of the requirements to design principles of Internet governance to steer the development and harmonization of standards and public policies emerged. The OECD, the Council of Europe, and the European Union, among others, designed numerous initiatives to determine such principles. The same reasoning prevailed in Brazil, in the drafting of the Internet Regulatory Framework. Both the Internet Regulatory Framework and the principles for Internet Governance and use in Brazil, prepared by the Brazilian Internet Steering Committee (CGI.br), have substantiated debates at the international level.

In addition, there is a more evident trend towards privatizing Internet governance, given the fragmentation of the network into closed platforms operating in private systems, such as social networks. The convergence between platforms accentuates this situation and leaves users vulnerable to decisions made unilaterally by businesses on important issues, such as their privacy policies. On the other hand, some private players, such as ISPs and domain names organizations, have been increasingly pressured to act as user-behavior Internet watchdogs and actively work to curb reputedly illegal conduct, in a process of privatization and outsourcing of law enforcement.

In 2011, a process of reopening discussions by some of the main institutions related to Internet governance began. The UN General Assembly decided to renew the Internet Governance Forum's (IGF) mandate until 2015, and a work group was created to come up with suggestions to improve the forum. The Internet Corporation for Assigned Names and Numbers (ICANN) also underwent a process of administrative reform and elected a new CEO. The implementation of the controversial decision to create new top level domain names, or gTLDs, is still ongoing.

Given this combination of factors, it is possible to predict greater social concerns on Internet governance, particularly in ensuring that established rights are respected on the network. One can even predict increased government involvement in this issue and a possible attempt to deepen dialogue with private players, particularly businesses.

6.3 Initiatives for the design of Internet governance principles

There is a consensus emerging in the international arena of the need to develop a harmonic framework of general principles before endorsing regulation on specific Internet-related issues. This list of common principles would help promoting convergence among actors and steering international standards. Drawing a parallel with the political processes that occur at the national level, some even claim that the Internet is going through a "constitutional" period, since the principles being discussed today may be the basis for the normative framework that will apply to the networked society of the future.[78]

6.3.1 CGI.br's principles for Internet use and governance in Brazil

The Brazilian Internet Steering Committee is a pioneering and unique experiment. Comprised by members from the government, the business sector, the third sector, and the academic community, the CGI.br is a model of democratic plural governance in which representatives from each non-governmental segment are elected to form a collective body that coordinates and integrates Internet service initiatives in the country.

The CGI.br also pioneered the debate on Internet principles. In 2009, considering the need to anchor their actions and decisions on solid foundations, the CGI.br adopted the following principles for governance and use of the Internet in Brazil:[79]

[78] IGF workshop 144: *Human Rights Come First: a Constitutional Moment for Internet Governance?* Nairobi, 2011. Available at: <http://www.intgovforum.org/cms/component/content/article/71-transcripts-/815-ig4d-workshop-144-human-rights-come-first-a-constitutional-moment-for-internet-governance>. Accessed on 20.07.12.

[79] CGI.br. Princípios da para a governança e uso da Internet no Brasil. RES/2009/003/P. Available at: <http://www.cgi.br/regulamentacao/resolucao2009-003.htm>. Accessed on 20.07.12.

1. Freedom, privacy and human rights

Internet use should be steered by the principles of freedom of expression, individual privacy, and human rights, acknowledging that these are essential to ensuring a just and democratic society.

2. Democratic and collaborative governance

Internet governance should be transparent, multilateral and democratic, involving various sectors of society, thus ensuring and promoting its collective creation nature.

3. Universality

Internet access must be universal for it to be a means of social and human development, contributing to building an inclusive and non-discriminatory society that benefits all.

4. Diversity

Cultural diversity must be respected and preserved, and its expression should be encouraged, refraining from imposing beliefs, customs or values.

5. Innovation

Internet governance should promote ongoing development and widespread availability of new use and access technologies and models.

6. Network neutrality

Filtering privileging traffic must only respect technical and ethical criteria; political, commercial, religious, cultural, or any other form of discrimination or favoritism is not permissible.

7. Network non-liability

Combating illicit behavior on the network must affect those actually responsible and not the means or vehicle of access. Furthermore, it must always respect the highest principles of protection of freedom, privacy and human rights.

8. Functionality, security, and stability

The stability, security and overall functionality of the network must be actively preserved, through technical measures consistent with international standards and promotion of best practices.

9. Standardization and interoperability

The Internet should be based on open standards that enable interoperability and the participation of all in its development.

10. Legal and regulatory environment

The legal and regulatory environment must preserve the dynamics of the Internet as a collaborative space.

This list of principles was presented to Internet Governance Forum (IGF) participants as a contribution from Brazil to the global debate on principles and was widely accepted. Markus Kummer, former Executive Secretary of the IGF, asserted: ""I could imagine an emerging consensus around these core principles. I for myself would happily endorse them." Vint Cerf added: "These are principles that I think could be widely and generally accepted."[80]

The document prepared by the CGI.br was one of the stimuli for initiatives aimed at developing the principles that have emerged since then.

6.3.2 Principles designed by the Council of Europe (CoE)

The Council of Europe – CoE is an international organization that promotes cooperation between European countries for the enforcement of human rights, democracy and the rule of law. It was founded in 1949 and has 47 member States. Among the CoE's institutional bodies there is the European Court of Human Rights, responsible for enforcing the European Convention on Human Rights, and the Committee of Ministers, which produces statements and recommendations that, albeit non-binding, carry significant political weight – i.e. characteristic of soft law instruments.

In 2005, CoE member States decided to analyze the feasibility of a legal instrument that could address cross-border Internet traffic. With this objective, they created an *ad hoc*, multi-stakeholder group of experts that proposed ten principles for Internet governance[81], endorsed in the joint statement by the CoE and the Committee of Ministers.[82] In addition to its emphasis on the protection of fundamental rights, some other principles are worth noting.

First of all, it argues that any policy applied to the Internet must recognize its global nature and respect the unrestricted flow of cross-border traffic on the

---

[80] Transcripts from the section *Taking stock of Internet governance and the way forward*. IGF 2010, Vilnius. Available at: <http://www.intgovforum.org/cms/component/content/article/102-transcripts2010/687-taking-stock>. Accessed on 20.07.12.

[81] Council of Europe ad hoc Advisory Group on Cross-border Internet. *Proposal for a draft Council of Europe Committee of Ministers Declaration on Internet Governance Principles*. Available at: <http://www.coe.int/t/dghl/standardsetting/media-dataprotection/conf-internet-freedom/Internet%20Governance%20Principles.pdf>. Accessed on 20.07.12.

[82] Council of Europe. *Declaration by the Committee of Ministers on Internet governance principles.* Adopted by the Committee of Ministers on September 21, 2011. Available at: <https://wcd.coe.int/ViewDoc.jsp?id=1835773>. Accessed on 20.07.12.

network. This general principle is supported by others, such as respect for openness, interoperability and the "end-to-end" nature of the Internet, as well as by the promotion of network neutrality.

Second of all, the document takes a stance on important issues related to Internet governance implementation. It states that "the private sector should retain its leading role in technical and operational matters," but that is also must ensure "transparency and accountability to the global community for those actions which impact on public policies."

Its multi-stakeholder nature is identified as key to ensuring the stability and resilience of the Internet. Most initiatives that aim to create a list of principles support a multi-stakeholder system, but, interestingly, the members of the ad hoc group of the CoE focused on debating a current and challenging theoretical topic: the relationship between the eminently intergovernmental international system and the Internet's multi-stakeholder governance model. According to Wolfgang Kleinwächter, member of the ad hoc group, "our conclusion, in the very early days the work of the group, was that we will continue to have a multilateral treaty system. But the multilateral treaties in the future will probably be embedded in a multi-stakeholder environment. That means the multi-stakeholder principle, you know, it's more or less the more general principle. And from this approach, then you can go to the specific rights".[83]

Thus, it is possible to predict a complementary relationship between hard law and soft law and interdependence between groups of players. Also according to Kleinwächter, the approach through non-binding soft law, as in the case of the CoE's declaration of principles, has the advantage of quickly reaching a convergent understanding. The document would not signify an end result, but a starting point for collaborative and multi-stakeholder debate.[84]

Parallel to the debate on principles, the Committee of Ministers of the CoE warned member states about threats to freedom of expression and association on the Internet that can result from the political pressure currently exerted on

---

[83] Wolfgang Kleinwächter. Transcripts from the 203 Workshop of the IGF 2011. *Internet Governance Principles: Initiatives Toward the Improvement of a Global Internet Governance.* Nairobi, 2011. Available at: <http://www.intgovforum.org/cms/component/content/article/71-transcripts-/912-ig4d-workshop-203-internet-governance-principles-initiatives-toward-the-improvement-of-a-global-internet-governance>. Accessed on 20.07.12.

[84] Idem.

Internet service providers and online platforms to make them act as co-agents of law enforcement. The Committee also expressed its concern about the curtailment of freedom of expression caused by attacks on independent media websites, on leak sites (such as WikiLeaks) and on human rights defenders and political dissidents. They agreed on a joint statement highlighting the important role of these players as facilitators of the enforcement of the rights to freedom of expression and freedom of association.[85]

6.3.3 The European Commission and the "Internet Compact"

The European Commission designs policies on issues related to the Internet through the Directorate General for Communications Networks, Content and Technology, whose expertise covers a wide range of issues, such as infrastructure and telecommunications, e-government, online education, digital content, among others. In the context of Internet governance, the Commission has been a major player, actively participating in the debate on institutional arrangements.

In 2011, during the high-level meeting of the OECD on Internet economy, the vice president of the European Commission, Neelie Kroes, argued that the "Academia, the private sector and civil society have contributed enormously to the success of the Internet. Politicians like me should be mindful of that. But public authorities neither can nor should take a back seat. The fact is that the Internet is of relevance and benefit for citizens, for the economy, and for society. For that reason alone it is of interest to public policy makers. One of the challenges is to respond to that legitimate interest, without damaging the very features of the Internet".[86]

According to the Commissioner, the Internet should remain as intervention-free as possible. Regulation should be seen as a last resort, and the role of the

---

[85] Council of Europe. *Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers*. Adopted by the Committee of Ministers on December 7, 2011. Available at: <https://wcd.coe.int/ViewDoc.jsp?id=1883671&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383>. Accessed on 20.07.12. Translation to Portuguese available at: <http://observatoriodainternet.br/conselho-da-europa-alerta-sobre-ameacas-a-liberdade-de-expressao-on-line>. Accessed on 20.07.12.

[86] Neelie Kroes. *OECD High Level Meeting on the Internet Economy*. Paris, June 28, 2011. Available at: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/479&format=HTML&aged=0&language=EN&guiLanguage=en>. Accessed on 20.07.12.

principles would indicate the essential elements of the Internet that should be promoted and preserved.[87] The European Commission issued a draft list of principles known as the Digital Compact for the Internet (in English, "compact" is the acronym of the first letters of each of the principles). This initiative was formally presented at the 2011 Internet Governance Forum in Nairobi, and addresses important issues, such as the need to preserve the fundamental characteristics of the network architecture, the need to avoid fragmentation and the need to use of the Internet to strengthen democracy. Briefly, the principles are as follows:

Civic Responsibility: As in offline society, on the Internet people have responsibilities to each other which are not just legal responsibilities.

One Internet. Fragmentation must be avoided.

Multi-stakeholder. The participation of all stakeholders in policy making is good.

Pro-democracy. With the right tools, the Internet can become an instrument to support democratic life.

Architecturally sound. The architecture of the Internet is fundamental to its dynamics. The architecture will change in the future as new challenges emerge, but we need to be aware of the implications that different models might have.

Confidence inspiring. Barriers to confidence are barriers to access. If we do not solve problems like protection of personal data, privacy and security, then people will be turned off the net.

Transparent Governance. This is the support base for the multi-stakeholder model. In particular, we need to be transparent about the role which governments, representing their citizens, play and ensure that those views are not ignored.

During her speech at the IGF 2011, Commissioner Neelie Kroes made some observations on the multi-stakeholder model and warned of the risks of multi-stakeholder spaces being taken over by private interests. "Ultimately, different actors have different fields of expertise and responsibility… public authorities have a particular role, indeed a particular obligation, to deal with public policy matters, off and on-line, and this must be reflected in the decision-making

[87] Neelie Kroes. Opening ceremony of the Internet Governance Forum. Nairobi, 2011. Available at :<http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/605&format=HTML&aged=0&language=EN&guiLanguage=en>. Accessed on 20.07.12.

process. Otherwise, the outcome of the multi-stakeholder approach is that lobbyists hijack decision-making, that private vested interests trump the public interest".[88]

The European Commission seems to be one of the stakeholders supporting an overhaul in Internet governance mechanisms, particularly to increase government participation: "we are not suggesting that some alternative to the multi-stakeholder model of Internet Governance is needed, just that it needs to be amended to function better and take into account the voice of Governments."[89] Considering the major releases and documents produced by the Commission, its positioning on governance mechanisms seems to be aimed at reviewing and expanding the scope of government participation in ICANN.[90]

The European Commission's initiative to outline principles is very welcome considering the EU's complex political and institutional map. However, unlike other countries that, in recent years, have begun adopting measures for Internet regulation, the EU and various member States already have a robust regulatory system on the issue, as well as consolidated practices that may impede definite implementation of the principles.

For example, it may be a challenge to reconcile the principle of preservation of the architecture with evidence that telecom operators restrict Internet access to their users, thus violating network neutrality.[91] According to La Quadrature du Net, free speech, privacy, innovation and competition are being harmed by such carrier practices.[92] Similarly, one can predict conflicts between principles aimed at promoting users' trust and the fear caused by an environment of constant surveillance, created by the approval of laws such as the Hadopi in France (Topic 9.3.1), which foresees the blocking of Internet access to repeat-offenders who download protected or copyrighted material.

---

[88] Idem.

[89] Neelie Kroes. *European Dialogue on Internet Governance (EuroDIG)*. Belgrade, 2011. Available at: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/419>. Accessed on 20.07.12.

[90] Kieren McCarthy. *European Commission Papers on ICANN: what they actually say*. Available at: <http://news.dot-nxt.com/2011/08/31/ec-papers-details>. Accessed on 20.07.12.

[91] La Quadrature du Net. Available at: <https://www.laquadrature.net/en/Net_neutrality>. Accessed on 20.07.12.

[92] Available at: <https://www.laquadrature.net/en/more-than-half-of-the-eu-with-restrictions-to-net-access-what-will-neelie-kroes-do>. Accessed on 20.07.12.

6.3.4 The United States and the International Strategy for the Cyberspace

In May 2011, president Barack Obama announced a strategic plan for the cyberspace with principles to guide the development of transversal Internet-related policies within the U.S. government.[93] The initiative's main focus is on security: the document acknowledges the role played by the Internet in economic and social development, but also the new threats that are perpetuated through the network. Among them, there are "natural disasters, sabotage, theft of intellectual property and potential threats that may endanger international peace and security".

The document states the government's intention to seek a balance between freedom and security in all government policies: "good cybersecurity can enhance privacy, and effective law enforcement targeting widely-recognized illegal behavior can protect fundamental freedoms". One of the U.S. government's international goals would be to increase the number of countries that adhere to the Budapest Convention on cybercrime.

The document highlights the role of proprietary and open software in the economy and in ensuring that all user needs are met, and it draws attention to the importance of interoperability and preservation of the end-to-end architecture to avoid network fragmentation. It states that "one country's method for blocking a website can cascade into a much larger, international network disruption." However, the document does not say that the U.S. government intends to change its own policy of seizing websites, which has caused international ripples.[94]

The importance of multi-stakeholder participation in Internet governance is highlighted throughout the document. The U.S. government recognizes the significance of the IGF and forums "that represent the entire Internet community by integrating the private sector, civil society, academia, as well as governments in a multi-stakeholder environment." Furthermore, it places special emphasis on the importance of government/private sector partnerships, suggesting that these actors' participation in planning governance is strategically important to

---

[93] *International strategy for cyberspace: prosperity, security and openness in a networked world*. May, 2011. Available at: <http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf>. Accessed on 20.07.12.

[94] Ars Technica. *Senator: domain name seizures "alarmingly unprecedented"*. Available at: <http://arstechnica.com/tech-policy/news/2011/02/senator-us-domain-name-seizures-alarmingly-unprecedented.ars>. Accessed on 20.07.12.

the U.S. government: "Although the private sector already plays an important role in international and multi-stakeholder organizations, we will continue to leverage existing partnership mechanisms to engage with industry partners. In particular, we will work closely with infrastructure owners and operators (…). We also seek the private sector's participation in Internet governance as essential to upholding its multi-stakeholder character, and will continue to advocate for inclusiveness in fora that take up such issues."

Finally, the document lists the priority policies for the U.S. government:

Economy: promoting international standards, and open and innovative markets

- Sustaining a free-trade environment that encourages technological innovation on accessible, globally linked networks;
- Protecting intellectual property, including commercial trade secrets, from theft;
- Ensuring the primacy of interoperable and secure technical standards, set forth by technical experts.

Protecting our networks: enhancing security, reliability and resilience

- Promoting cyberspace cooperation, particularly on codes of conduct for States and cybersecurity, bilaterally and in a range of multilateral organizations and multinational partnerships;
- Reducing intrusions into and disruptions of U.S. networks;
- Ensuring robust incident management, resilience and recovery capabilities for the information infrastructure;
- Improving the security of the high-tech supply chain.

Law enforcement: extending collaboration and the rule of law

- Participating fully in international cybercrime policy development;
- Harmonizing cybercrime laws internationally by promoting endorsement of the Budapest Convention;
- Focusing cybercrime laws on combating illegal activities, without restricting access to the Internet;
- Denying terrorists and other criminals the ability to exploit the Internet for implementing planning, financing or attacks.

Military: preparing for 21st century security challenges

- Recognizing and adapting to the increasing military need for reliable and secure networks;
- Building and enhancing existing military alliances to confront potential threats in cyberspace;
- Expanding cyberspace cooperation with allies and partners to increase collective security.

Internet Governance: promoting effective and inclusive structures

- Prioritizing openness and innovation on the Internet;
- Preserving global network security and stability, including the domain name system (DNS);
- Promoting and enhancing multi-stakeholder forums for debating Internet governance issues.

International Development: training, security and prosperity

- Providing the necessary knowledge, training and other resources to countries seeking to build technical and cybersecurity capacity;
- Frequent designing and regular sharing of international cybersecurity best practices;
- Enhancing States' ability to fight cybercrime; including training for law enforcement, forensic specialists, jurists and legislators;
- Developing relationships with policymakers to enhance technical qualification, providing regular and ongoing contact with experts and their United States Government counterparts.

Freedom on the Internet: supporting fundamental freedoms and privacy

- Supporting civil society players to create reliable, secure and safe platforms for freedom of expression and association;
- Collaborating with civil society and non-governmental organizations to establish safeguards protecting their Internet activity from unlawful digital intrusions;
- Encouraging international cooperation for effective commercial data privacy protections;
- Ensuring end-to-end interoperability in an Internet accessible to all.

6.3.5 Discussions on the principles within the G8

In 2011, for the first time, the G8 addressed Internet governance at its summit level, which brings together Heads of State and Government leaderships. The final declaration of the G8 summit[95] listed a series of principles discussed in the e-G8 event held before the official summit. The e-G8 included the participation of representatives of major Internet companies. However, civil society had little chance of involvement, which drew criticism that the event "jettisons the

[95] Declaration of the G8. *Renewed Commitment For Freedom And Democracy*. Deauville Summit. May, 2011. Available at: <http://www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html>. Accessed on 20.07.12.

principle of multi-stakeholder participation that has evolved globally,"[96] and emphasized that "policies framed together by the most powerful nations, quite likely, will become the default global norm (...). It is, therefore, appropriate that G8 countries engage with the same and other issues of Internet policies at the more democratic global forums where all countries are present at an equal".[97]

Civil society organizations attending the e-G8 noted that the message sent by the event was dubious. If, on the one hand, it addressed important principles such as freedom of expression, respect to privacy, and multi-stakeholder participation, on the other hand, its emphasis on combating cybercrime and protecting intellectual property online lacked both a clear means to be used for this purpose and assessment on how such actions would impact on access and free data traffic on the network.

The Article 19 organization stated that the declaration did not acknowledge human rights protection "as a core principle above all others", and placed more emphasis on economic concerns, particularly the protection of intellectual property, in that it seems to endorse new restrictions on freedom of expression on the Internet, strengthening enforcement of intellectual property rights and moving towards controversial proposals, such as the Anti-counterfeiting Trade Agreement – ACTA and national laws providing for a progressive or three strikes response.[98]

There was no direct reference to the importance of the principle of network neutrality or the role that large companies, many of which based in developed countries, play in censorship policies and enforcement. Without addressing these issues, the G8 discussions seem little inclined to make a positive tangible impact on promoting rights and freedom of expression on the Internet.

---

[96] Internet Governance Caucus. *Open letter to President Sarkozy on eG20 meeting plan*. Available at: <http://www.igcaucus.org/open-letter-president-sarkozy-eg8-meeting-plan>. Accessed on 20.07.12.

[97] Idem.

[98] Article 19. "*G8: the Deauville Declaration on Internet Fails to Recognise Importance of Human Rights Including Freedom of Expression*. Available at: <http://www.article19.org/data/files/pdfs/press/g8-the-deauville-declaration-on-internet-fails-to-recognise-importance-of-hu.pdf>. Accessed on 20.07.12.

TABLE 1. COMPARISON OF PRINCIPLES OF THE CGI.BR, THE BRAZILIAN INTERNET REGULATORY FRAMEWORK, THE DECLARATION OF THE COUNCIL OF EUROPE (JUNE 2011), THE OECD REPORT (JULY 2011), THE INTERNATIONAL U.S. STRATEGY FOR CYBERSPACE (MAY 2011), THE EU PROPOSAL (JULY 2011), AND THE DECLARATION OF THE G8 (MAY 2011). ADAPTED FROM WOLFGANG KLEINWÄCHTER – INTERNET PRINCIPLE HYPE. POLITICS MAGAZINE NO. 10 – AUGUST, 2011.

Topic	CGI.br	Brazilian Internet Regulatory Framework (PL 2126/2011)	CoE	OECD	USA	EU	G8
Human Rights	[1] Freedom, privacy and human rights	[article 2, II] Human rights and citizenship [article 2, III] Plurality and Diversity [article 3, I and II, article 7, Single paragraph, article 8, article 10] Protection of privacy and personal data [article 3, III] Freedom of expression, communication, and manifestation [article 7, I] Communication inviolability and privacy [article 7 o, II] no-interruption of connection [article 7o, III] Service level seamlessness [article 7, IV] Access to clear and complete information contained in service contracts [article 7, V] no disclosure to third-parties of connection and access to Internet applications records [article 19, VIII] promotion of culture and citizenship	[1] Human rights, democracy and laws	[1] Free global traffic of information	[1]Support to fundamental freedoms	[4] Pro-democracy	[1] Freedom
	[5] Cultural diversity		[10] Linguistic and cultural diversity	[9] Protection of privacy	[3] Valuing privacy		[2] Protection of privacy

TABLE 1. COMPARISON OF PRINCIPLES OF THE CGI.BR, THE BRAZILIAN INTERNET REGULATORY FRAMEWORK, THE DECLARATION OF THE COUNCIL OF EUROPE (JUNE 2011), THE OECD REPORT (JULY 2011), THE INTERNATIONAL U.S. STRATEGY FOR CYBERSPACE (MAY 2011), THE EU PROPOSAL (JULY 2011), AND THE DECLARATION OF THE G8 (MAY 2011). ADAPTED FROM WOLFGANG KLEINWÄCHTER – INTERNET PRINCIPLE HYPE. POLITICS MAGAZINE NO. 10 – AUGUST, 2011. (CONTINUATION)

Topic	CGI.br	Brazilian Internet Regulatory Framework (PL 2126/2011)	CoE	OECD	USA	EU	G8
Security	[7] Network non-liability	[article 3, VI] Agents accountability based on their activities [article 14]. Internet connection providers are not accountable for damage resulting from content generated by third-parties [article 15] Internet application providers may only be held accountable for content generated by third parties if, after legal rulings, they do not take appropriate action to make the infringing content unavailable	[3] Responsibility of States	[5] Reliable database for policy making	[4] Protection against crimes	[1] Civic responsibility	[2] Cybersecurity
			[6] Integrity and the Internet	[6] Transparency, due legal proceedings and accountability	[5] Right to self-defense		[3] Protection against crimes
				[13] Cooperation for Internet security	Cybersecurity and thorough investigation		

TABLE 1. COMPARISON OF PRINCIPLES OF THE CGI.BR, THE BRAZILIAN INTERNET REGULATORY FRAMEWORK, THE DECLARATION OF THE COUNCIL OF EUROPE (JUNE 2011), THE OECD REPORT (JULY 2011), THE INTERNATIONAL U.S. STRATEGY FOR CYBERSPACE (MAY 2011), THE EU PROPOSAL (JULY 2011), AND THE DECLARATION OF THE G8 (MAY 2011). ADAPTED FROM WOLFGANG KLEINWÄCHTER – INTERNET PRINCIPLE HYPE. POLITICS MAGAZINE NO. 10 – AUGUST, 2011. (CONTINUATION)

Topic	CGI.br	Brazilian Internet Regulatory Framework (PL 2126/2011)	CoE	OECD	USA	EU	G8
Governance	[2] Democratic and collaborative governance	[article 3, VII] Preservation of the participative nature of the network [article 19, I] establishing a mechanism for transparent, collaborative and democratic governance, with the participation of various sectors of society	[3] Multi-stakeholder Governance	[5] Multi-stakeholder processes for policy-making	[9] Multi-sectorial governance	[3] Multi-sectorial governance	[4] Multi-sectorial governance
			[4] Empowering users	[6] Voluntarily designed codes of conduct		[7] Transparent governance	
	[10] Legal and regulatory environment – should preserve the Internet as a collaborative space		[7] Decentralized management	[10] Empowerment and responsibility of individuals			
				[14] Implementation and enforcement of regulations			

TABLE 1. COMPARISON OF PRINCIPLES OF THE CGI.BR, THE BRAZILIAN INTERNET REGULATORY FRAMEWORK, THE DECLARATION OF THE COUNCIL OF EUROPE (JUNE 2011), THE OECD REPORT (JULY 2011), THE INTERNATIONAL U.S. STRATEGY FOR CYBERSPACE (MAY 2011), THE EU PROPOSAL (JULY 2011), AND THE DECLARATION OF THE G8 (MAY 2011). ADAPTED FROM WOLFGANG KLEINWÄCHTER – INTERNET PRINCIPLE HYPE. POLITICS MAGAZINE NO. 10 – AUGUST, 2011. (CONTINUATION)

Topic	CGI.br	Brazilian Internet Regulatory Framework (PL 2126/2011)	CoE	OECD	USA	EU	G8
Technology/ architecture	[3] Universality	[article 2, IV] Openness and Collaboration [article 3, IV] Network neutrality [article 3, V] Stability, security, and functionality [article 9] Those responsible for transmission, switching and routing have the duty of treating any data packets isonomically, regardless of content, origin and destination, service, terminal, or application, and no form of discrimination or degradation of traffic not resulting from technical requirements needed to provide adequate services, is allowed, in accord with regulations	[5] Universality of the Internet	[2] Open distributed, and interconnected Internet	[6] Global interoperability	[2] One Internet	
	[6] Network neutrality		[8] open architecture		[7] Network stability	[5] Open architecture	
	[8] Functionality, security and stability		[9] open network		[8] Reliable access		
	[9] Standardization and interoperability						

TABLE 1. COMPARISON OF PRINCIPLES OF THE CGI.BR, THE BRAZILIAN INTERNET REGULATORY FRAMEWORK, THE DECLARATION OF THE COUNCIL OF EUROPE (JUNE 2011), THE OECD REPORT (JULY 2011), THE INTERNATIONAL U.S. STRATEGY FOR CYBERSPACE (MAY 2011), THE EU PROPOSAL (JULY 2011), AND THE DECLARATION OF THE G8 (MAY 2011). ADAPTED FROM WOLFGANG KLEINWÄCHTER – INTERNET PRINCIPLE HYPE. POLITICS MAGAZINE NO. 10 – AUGUST, 2011. (CONTINUATION)

Topic	CGI.br	Brazilian Internet Regulatory Framework (PL 2126/2011)	CoE	OECD	USA	EU	G8
Economy	[5] Innovation	[article 2, V] free initiative, free competition and consumer protection [article 19, VI] optimization of the network infrastructure, promoting technical quality, innovation and widespread availability of Internet applications, without prejudice to its openness, neutrality and participative nature;		[3] Investment and competitiveness in broadband and high speed services [15] Delivery of cross-border services [11] Creativity and innovation [12] Limits for intermediary responsibilities and requirements	[2] Respect to property	[6] Reliability for users	[3] Protection of intellectual property

TABLE 1. COMPARISON OF PRINCIPLES OF THE CGI.BR, THE BRAZILIAN INTERNET REGULATORY FRAMEWORK, THE DECLARATION OF THE COUNCIL OF EUROPE (JUNE 2011), THE OECD REPORT (JULY 2011), THE INTERNATIONAL U.S. STRATEGY FOR CYBERSPACE (MAY 2011), THE EU PROPOSAL (JULY 2011), AND THE DECLARATION OF THE G8 (MAY 2011). ADAPTED FROM WOLFGANG KLEINWÄCHTER – INTERNET PRINCIPLE HYPE. POLITICS MAGAZINE NO. 10 – AUGUST, 2011. (CONTINUATION)

Topic	CGI.br	Brazilian Internet Regulatory Framework (PL 2126/2011)	CoE	OECD	USA	EU	G8
The principles below are present in the Brazilian Internet Regulatory Framework, but are not part of the initial parameters of comparison between the proposed principles, which is why they appear separate from the others.							
e-Government/ Open Government		[article 19, II, III] Technological interoperability of e-government services, between the different powers and levels of the federation Interoperability between the various systems and terminals, including between the various sectors of society [article 19, IX; article 20, IV] Provision of public services to citizens in an integrated, efficient, and simplified manner via multiple access channels [article 20, I] Compatibility of e-government systems with various terminals, operating systems and applications [article 20, III] Compatibility with both human and automated information processing [article 20, V] Strengthening of social engagement in public policies					

TABLE 1. COMPARISON OF PRINCIPLES OF THE CGI.BR, THE BRAZILIAN INTERNET REGULATORY FRAMEWORK, THE DECLARATION OF THE COUNCIL OF EUROPE (JUNE 2011), THE OECD REPORT (JULY 2011), THE INTERNATIONAL U.S. STRATEGY FOR CYBERSPACE (MAY 2011), THE EU PROPOSAL (JULY 2011), AND THE DECLARATION OF THE G8 (MAY 2011). ADAPTED FROM WOLFGANG KLEINWÄCHTER – INTERNET PRINCIPLE HYPE. POLITICS MAGAZINE NO. 10 – AUGUST, 2011. (CONTINUATION)

Topic	CGI.br	Brazilian Internet Regulatory Framework (PL 2126/2011)	CoE	OECD	USA	EU	G8
Accessibility		[article 20, II] Accessibility for all interested parties, regardless of their physical/motor, perceptive, cultural, and social abilities					
Development of Capacities		[article 19, VII] development of Internet training actions and programs [article 21] Fulfillment of the state's Constitutional requirement to provide education at all levels, which includes training for safe, conscientious and responsible use of the Internet as a tool for citizenship and to promote cultural and technological development					

6.4 Improving the Internet Governance Forum (IGF)

The IGF is one of the key results of the World Summit on the Information Society's (WSIS) discussion, held in two stages in 2003 and 2005.[99] The participants urged the UN Secretary General to create, through an open and inclusive process, a new forum for multi-stakeholder policy debate related to the network.[100] The IGF is now the main forum in which discussions occur transversally on a wide range of issues such as access, privacy, security, and openness.

The IGF's multi-stakeholder feature means that governments, civil society, academia, the technical community, and the business sector jointly participate on equal terms in the forum's discussions. Thus, the IGF creates opportunities for synergy, for identifying emerging topics and consolidating partnerships.

The IGF was held in Greece (2006), Brazil (2007), India (2008), Egypt (2009), Lithuania (2010) and Kenya (2011). After five years, the forum's initial mandate ended, but it was renewed until 2015. According to the UN General Assembly resolution[101], the forum must be improved to align it with the debate on global Internet governance.

The process of discussion on improving the IGF was led by the UN Commission on Science and Technology for Development (CSTD), which created a working group to seek, compile and analyze contributions by all member States and all other stakeholders and to make recommendations.[102]

The Working Group's discussions were grouped into themes: 1) results of the IGF discussions; 2) working arrangements, including open consultations, functioning of the Secretariat, and the role of the Multi-stakeholder Advisory Group – MAG; 3) IGF financing; 4) increased participation; and 5) links between the IGF and other processes, mechanisms, and bodies dealing with issues related to Internet governance.

---

[99] *World Summit on the Information Society*. Available at: <http://www.itu.int/wsis/index.html>. Accessed on 20.07.12.

[100] Tunis Agenda (paragraph 72), endorsed. Resolution 60/252 of the UN General Assembly.

[101] Available at: <http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan039074.pdf>. Accessed on 15.08.12.

[102] Work group on improving the IGF. Available at: <http://www.unctad.info/en/CstdWG/>. Accessed on 20.07.12.

The working group met during 2011 and should complete its report in 2012, submitting it to the UN Economic and Social Council (ECOSOC). During the discussions, important consensuses were reached, such as a general understanding that the IGF should produce more concrete results – capturing the convergences and different views on specific issues related to public policies – that may be shared with stakeholders and organizations relevant to the Internet governance system.

It was agreed that there should be measures aimed at increasing forum participation, particularly by players from developing and less advanced countries. Remote participation was recognized as part of the IGF's dynamics, as was the need for providing it with resources to make it fully operational. However, the forum's financing model, based only on voluntary donations, will remain the same, which could limit the implementation of these suggestions for improvement.

6.5 Pressures towards implementation of the improved cooperation mechanism, presented the Tunis Agenda of the World Summit on the Information Society

Enhanced cooperation was a result of discussions at the World Summit on the Information Society (WSIS). In accordance with paragraph 69 of the Tunis Agenda, it would be a mechanism "to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet, but not in the day-to-day technical and operational matters, that do not impact on international public policy issues."

The vague definition of enhanced cooperation provided in the Tunis Agenda has led to disagreements on mechanism implementation. Some players believe that it should translate into a more formal and close coordination between the organizations dealing with governance-related issues. Other players advocate that the issues be discussed in an existing or yet to be created multilateral forum within the UN. They argue that decisions on Internet-related public policies are currently being made in forums with limited participation – such as the OECD or the Council of Europe – in which developing countries are not present.

The discussion about enhanced cooperation has intensified since 2010, when a series of consultations and meetings were held by the UN Department of Economic and Social Affairs – UN DESA. Recently, a series of meetings to

reconcile positions on the issue was scheduled for 2012, under the UN Science and Technology Commission in Geneva. Meanwhile, countries with various political and ideological regimens have sought to expound their positions and outline, albeit generally, their understandings of the role of the State and multilateral bodies in Internet governance. Various documents produced recently have, explicitly or implicitly, discussed enhanced cooperation and should be interpreted within this political context.

6.6 The international code of conduct on information security proposed by China, Russia, Tajikistan and Uzbekistan

The draft resolution A/66/359[103] was submitted to the UN member countries at the 66th UN General Assembly. The code of conduct should steer regulations to prevent the use of information technology and communications for purposes inconsistent with the objectives of maintaining international stability and security, which may adversely affect the integrity of the infrastructure in States, at the expense of security. Under the proposal, the code of conduct would be open to voluntary adhesion by the States wishing to be part of its jurisdiction.

If, on one hand, the proposed code states that countries must respect "human rights and fundamental freedoms", on the other, the document aims at "curbing dissemination of information which incites terrorism, secessionism, extremism or undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment." The generality of the text leaves ample room for repression against the legitimate exercise of freedom of expression and may constrain signatories in complying with legislative parameters more stringent than those currently in effect.

[103] *International Code of Conduct for Information Security*. Available at: <http://nz.chineseembassy.org/eng/zgyw/t858978.htm>. Accessed on 20.07.12.

6.7 The IBSA Forum on Internet Governance

IBSA is a permanent dialogue mechanism established in 2003 between India, Brazil and South Africa. Its main objectives are to promote political cooperation, seek the democratization of international forums (increasing the participation of developing countries), promote cultural, technical, and scientific cooperation, and implement measures to promote development.

The IBSA Forum on Internet Governance was held in September 2011 at the Getulio Vargas Foundation in Rio de Janeiro. The event was sponsored by the Ministry of Foreign Affairs and with the support of the Brazilian Internet Steering Committee (CGI.br) and the Center for Technology and Society (CTS/FGV). The purpose of the meeting was to discuss substantive issues and institutional arrangements on the agenda of Internet governance, in order to identify the interests and priorities of stakeholders from the three countries.

A general statement of reflections on socioeconomic development and Internet access, led to the discussion of specific issues, such as infrastructure, critical resources, regulatory principles and institutional arrangements. Other issues were highlighted as relevant and requiring further development, such as jurisdiction, e-commerce and tax issues, open standards, network neutrality and media convergence.

In discussions on institutional arrangements, the participants acknowledged the important role played by the IGF in Internet governance, as a space of awareness, training and identification of public policy issues. At the same time, some participants argued that the existing mechanisms do not implement the enhanced cooperation ideal, as described in the Tunis Agenda.

The Indian IT for Change organization contributed to the forum's discussions with an article highlighting some of the most important issues for developing countries:[104]

[104] IT for Change. *A Development Agenda in Internet Governance: Outlining Global Public Policy Issues and Exploring New Institutional Options*. Preliminary contribution to the IBSA seminar on global governance of the Internet. Available at: <www.culturalivre.org.br/artigos/dev_agenda_ig.pdf>. Accessed on 20.07.12.

Cross-Border and Jurisdiction Issues

Developing countries need to consider that the most important "nodes" of Internet traffic are in northern countries, leading to asymmetry on the applicability of network laws. For example, in the beginning of 2011, the U.S. government seized the domain name of the Spanish website Rojadirecta.org, which provided links for streaming of sporting events. It was based in Spain, basically catering to the local population. Its model was tested in Spanish courts a few time and found not in breach of Spanish law. However, the U.S. was able to seize the domain name and close the website simply because the domain name .org is run by a US registered entity. In architectural material, the U.S. has comparatively broad control of the global Internet, and its executive and judicial agencies are increasingly leveraging this control.

Intellectual property and access to knowledge

One of the most important characteristics of the Internet is that it offers a seamless platform for global sharing of information and knowledge. At the same time, knowledge has become the key resource to be controlled and manipulated for economic domination, which makes its control the key economic agenda of developed countries. The Internet is being used as an instrument of cross border enforcement of intellectual property rules in extra-legal ways, often through the use of invasive technology, technology protection measures (DRMs) or through the use of providers as a type of private police for intellectual property law enforcement.

Commerce and tax Issues

There are two kinds of commerce issues implicated here. One is the use of Internet only for making contact, interaction and payment, whereas goods are delivered physically. The second kind creates very significant new governance challenges. There have been numerous problems that have arisen in relation to application of consumer rights laws to remote sales. In addition, levying of legitimate taxes on such transactions is another important issue. While digital service exporting companies pay taxes in the jurisdiction of their location and registration, authorities in the country where consumption of services takes place find it difficult to levy their taxes on such transactions. Developed countries, such as the members of the European Union, have done considerable work towards rationalization of taxes applicable to such cross-border digital trade. However, developing countries are not part of any such arrangement. Things become much more complex when services are traded using private digital currencies, like Facebook Credits.

Interconnection regimens

Negotiating Internet connectivity between national and global networks is an important and complex issue, unfortunately left entirely to unregulated markets. Interconnection charges were recognized by the Tunis Agenda of the World Summit on the Information Society (WSIS) as key to development, but little has been done to date with regard to this issue.

Competition issues in the global digital industry

The global Internet industry is characterized by monopolies, because of the increasing large scale economies that are unique to this area. Microsoft, Google, Facebook, Twitter and Apple-iTunes are prime examples of this. There are no initiatives to deal with this anti-competitive behavior, through appropriate regulation: the global Internet industry is almost completely unregulated. Two important reasons for such a unsustainable situation are (1) global Internet companies are simply too powerful for any country, especially any developing country, to be effectively regulated, and (2) almost all of these companies are based in the North, chiefly in the U.S., and are a key piece of the controlling strategy based on intellectual property. No enforcement competition law means that the late entrants from developing countries to the global Internet Industry hardly stand a chance to be in the global plan, or even in their own countries, against the global monopolistic or oligopolistic companies. It is not only the technical architecture of the Internet whose openness has to be ensured, but also the architecture of the global Internet industry has to be kept sufficiently open.

Governance of global corporations

Platforms like Facebook and Twitter have been used for political activism. As such, their neutrality and commitment to freedom of expression becomes very important. Platforms and social networks have arbitrarily and randomly adopted different approaches in different contexts and countries. In addition, personal content placed on the network is increasingly becoming an important part of social life. Remedies against arbitrary acts by companies must be readily available to individuals, particularly for those based in other countries.

Network openness and neutrality and open standards

The Internet is a communication platform capable of bringing change and innovation, essentially because of its open architecture. However, this situation is changing. The basic Internet protocols are still open, but today's Internet is dominated by proprietary applications. A very large proportion of Internet traffic flows through just a handful of proprietary mega-digital spaces. Since mobile Internet architecture was built later, in a largely commercial environment, it is a much more closed and vertically integrated. The principle of Network Neutrality is rapidly being eroded, particularly in mobile Internet.

Security

Threats to security vis a vis the global Internet require an urgent and sustained global cooperation, which will require some kind of formalized means to do so. The security of infrastructures can be fatally hit through the Internet: in 2011, a virus was implanted remotely, apparently aimed at an Iranian nuclear facility. Analysts believe that if the attack had been successful, it may not only have crippled the nuclear plant, but could have also triggered a nuclear disaster. News of cyber-attacks on government systems and cases of industrial espionage are daily news today.

Media

The national media is an important institution for governance and democracy; it has emerged as a major platform for political mediation between governments and citizens, but this is changing rapidly with the advent of the Internet, IPTV and convergence. It may be true that the old regulations cannot be applied to the new Internet context and that new regulatory frameworks will be required. Some kind of global discussion and framework may be required. How can effective national media spaces be carved out and maintained within the global Internet? What are the structural implications of this on the national public sphere, on democratic institutions and on giving a voice to the marginalized? Who are the ones interested in global Internet governance issues? These are some of the key questions in the emerging context.

Cultural diversity

The Internet may be and environment with greatly reduced cost of content production and transmission and may represent great opportunity for promoting cultural diversity. This bespeaks the need for efficient polices and support to good practices.

6.8 Human rights development

Internet governance has profound implications for transversal issues of development and human rights. For developing countries, the importance of the Internet for economic, social, and human development is the determinant for their perspectives on Internet governance. However, development is not yet seen as a key issue in the context of governance. The Internet also significantly affects human rights – both positively and negatively. Much of the debate on these Internet rights is, almost exclusively, interpreted negatively, either in non-intervention in the individual realm or in civil and political rights. It is important to perceive the connection between the Internet and human rights in a more holistic way, considering its indivisibility. Economic, social, and cultural rights must be respected along with civil and political rights.

At the end of the IBSA seminar during an intergovernmental meeting, government representatives prepared a document[105] that would serve as an initial contribution to the discussion of enhanced cooperation. This

[105] Available at: <http://www.culturalivre.org.br/artigos/IBSA_recommendations_Internet_Governance.pdf>. Accessed on 20.07.12.

document was extensively discussed during the IGF 2011 in Nairobi, in which representatives of IBSA governments attended several sessions and workshops. The Brazilian government said that the document formulated during the seminar was open to suggestions and changes and that a proposal for enhanced cooperation would be made only after a discussion with all concerned sectors.

At the fifth IBSA summit in October 2011, the leaders of the three countries reaffirmed their pledge to seek joint positions on Internet governance-related issues, stressed the importance of implementing an enhanced cooperation mechanism, noted discussions held at the Rio de Janeiro seminar on Internet governance, and recommended establishing an observatory to monitor developments in the field of Internet governance, assisting in disseminating information and analyses among member countries.[106]

The leaders also addressed the issue of intellectual property protection, emphasizing the "need for a balanced international intellectual property system that contextualizes Intellectual Property Rights in the larger framework of socio-economic development and views them, not as ends in themselves, but as a means of promoting innovation, growth and development in all countries." In addition, they warned "against attempts at developing new international rules on enforcement of intellectual property rights outside the multilateral fora that may give free rein to systematic abuses in the protection of rights, the building of barriers against free trade and undermining fundamental civil rights".[107]

6.9 India's proposal to create UN Committee for Internet-related policies

At the 66th meeting of the UN General Assembly, India submitted a proposal to establish a Committee for Internet-related public policies. According to the Indian proposal, the Committee would have the following responsibilities:

---

[106] Fifth India-Brazil-South Africa (IBSA) Dialogue Forum. Tshwane Declaration, 2011. Available at: <http://www.itamaraty.gov.br/sala-de-imprensa/notas-a-imprensa/v-cupula-do-forum-de-dialogo-india-brasil-e-africa-do-sul-ibas-2013-18-de-outubro-de-2011-declaracao-de-tshwane>. Accessed on 20.07.12.

[107] Idem.

1. Designing and establishing international public policies with a view to ensure coordination and coherence in cross-border Internet-related global issues;
2. Coordinating and overseeing the bodies responsible for technical and operating functioning of the Internet, including setting global standards;
3. Facilitating the negotiation of treaties, conventions and agreements on Internet-related public policies;
4. Addressing developmental issues related to the Internet;
5. Promoting human rights protection, i.e. civil, political, social, economic and cultural rights, including the Right to Development;
6. Arbitrating and resolving disputes, where necessary; and
7. Managing Internet-related crisis.

The Committee would be comprised by 50 States and have five advisory committees, responsible for counseling and assisting governments. It would report directly to the UN General Assembly and make non-binding recommendations for consideration, adoption or implementation by intergovernmental bodies and international organizations. The committee is presented as an addition, not as a substitute to the IGF. The mechanism would be financed through a combination of UN funds and proceeds from domain names registration fees.

Anticipating criticism of the initiative, the Indian government stated that "the intent behind proposing a multilateral and multi-stakeholder mechanism is not to 'control the Internet' or allow governments to have the last word in regulating the Internet, but to make sure that the Internet is governed not unilaterally, but in an open, democratic, inclusive and participatory manner, with the participation of all stakeholders".[108]

[108] Milton Mueller. *A United Nations Committee for Internet-relates policies? A fair assessment.* Available at: <http://www.internetgovernance.org/2011/10/29/a-united-nations-committee-for-internet-related-policies-a-fair-assessment/>. Accessed on 20.07.12.

In fact, the document was criticized, primarily on the following aspects:

- The document could cause a reversal of the current multi-stakeholder model, relegating non-governmental players to the background;
- A duplicate forum could empty the IGF in the long term;
- The funding mechanism is not clear on whether an additional fee would be charged for domain name registrations or if some type of contribution would be imposed on the ICANN;
- The precise meaning of the power to "coordinate and oversee the bodies responsible for technical and operating functioning of the Internet" is not clear in the document. As identified in some analyzes, this power does not appear in the summary of the Committee's proposal, which raises questions on whether there was a real intention to include it.

Some have said it possible that such initiatives may lead to the emergence of a bipolar Internet governance system: one axis would be led by organically developed institutions with technical competence and would be multi-stakeholder; whereas, the other would be led by governments dealing with public policy issues. "What we may be seeing here is not a death-struggle between polar choices of governance regimes, but a parting of the ways between the governments and the ODII as they more or less get out of each other's way".[109]

Other analyzes argue for the relevance of the Indian proposal, primarily because they perceive an increased risk of the current system of governance being taken over by private interests of large companies. According to this positioning, it would be "naive (or dishonest)… to imagine that the Internet is currently governed by multi-stakeholder networks that are equally open to all stakeholders, and that the choice is between maintaining this decentralized and bottom-up regime of governance on the one hand, or handing over control to governments on the other. In fact, some of the most important areas of public policy online are not governed by multi-stakeholder networks at all, not even by any existing intergovernmental organizations, but by individual national governments and big businesses (...). The Indian proposal, on the other hand,

[109] Idem.

could at least democratize these decisions to some degree. If a UN Committee for Internet-Related Policies, adequately linked to multi-stakeholder public sphere, were able to set global norms for the Internet in an adequately open and inclusive manner.[110]

It is likely that the Indian proposal will be discussed again in 2012, when the Committee on Science and Technology for Development (UN CSTD) will hold a meeting on enhanced cooperation.

[110] IGF Watch. India's proposal for a UN Committee for Internet-Related Policies (CIRP). Available at: <http://igfwatch.org/discussion-board/indias-proposal-for-a-un-committee-for-internet-related-policies-cirp>. Accessed on 20.07.12.

7

E-Commerce

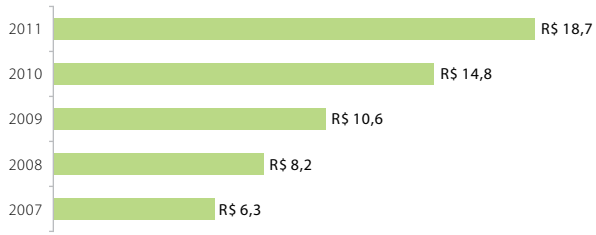
7.1 E-commerce and update of the Consumer Protection Code (CDC)

E-commerce refers to all commercial transactions carried out on the Web. Since the creation of the Internet, it has grown steadily to become an essential resource in daily life, reaching over 32.3 million single users, also called e-consumers[111], in October 2011. According to data from the 25th edition of the Webshoppers survey, conducted by the e-commerce company e-bit[112], e-commerce turnover rose from BRL 14.9 billion in 2010 to BRL 18.7 billion in 2011, a 26% increase compared to the previous year. The chart below shows the evolution of the sector's turnover between 2007 and 2011.

[111] Data obtained from article published in Jornal do Brasil online, available at: <http://www.jb.com.br/ciencia-e-tecnologia/noticias/2011/11/28/comercio-eletronico-atingiu-mais-de-32-milhoes-de-usuarios-em-outubro/>. Accessed on 02.03.12.

[112] Data available at: <http://www.webshoppers.com.br/webshoppers/WebShoppers25.pdf>. Accessed on 19.07.12.

E-COMMERCE TURNOVER EVOLUTION (IN BILLION BRL)



SOURCE: E-BIT INFORMAÇÃO (WWW.EBITEMPRESA.COM.BR)

Problems involving online shopping, however, have featured regularly in the media. These problems were reflected in the 2011 general complaints ranking of the Consumer Protection Agency (Procon)[113], in which the BW2 group, owner of the e-commerce companies Americanas.com, Submarino and Shoptime, ranks second among enterprises with the highest number of complaints. These companies received a total of 1,574 complaints, 620 of which went unanswered. This represents a substantial decline compared to the previous year, in which the group ranked 21st. The survey asserts, however, that this decline "reflects the growth of e-commerce, the sector through which many of the products receiving complaints last year were offered and acquired" (page 24).

In this context, e-commerce was selected as one of the key topics to be assessed by the Committee of Jurists specially constituted to amend the Consumer Protection Code (CDC) – Law 8,078, enacted in 1990. This process is necessary, therefore, to adjust consumer regulations to the new reality afforded by online purchasing, which is reflected in the sharp growth of e-commerce in the past years.

At the same time, in 2011 consumer protection agencies responded vigorously to the increase in complaints involving online shopping. The Procon of São Paulo, for example, opened an investigation into 20 websites offering e-commerce services[114] due to the great number of complaints of undelivered purchases. The investigations revealed that many suppliers, some registered as private individuals, could not be located at their official addresses. In the meantime, the Consumer Protection Center (Nudecon) of the Public Defender's Office of Rio de

[113] Available at: <http://www.procon.sp.gov.br/pdf/acs_ranking_2011.pdf>. Accessed on 17.07.12.

[114] Taken from the article: <http://economia.ig.com.br/financas/seunegocio/procon+sp+denuncia+fraudes+em+sites+de+comercio+eletronico/n1300142822745.html>. Accessed on 07.03.12.

Janeiro notified online sales and group buying sites to respond to consumers' complaints. Between August and December of that year, the number of online sales complaints filed at Nudecon increased by 60%.[115]

The issue has also reached the courts. According to data of the Federal Senate, a high rate of lawsuits involving consumer relations was verified in 2011, corresponding to approximately 20% to 30% of private law appeals filed at the Supreme Court of Justice. The advent of new forms of consumer relations that did not exist when the CDC was first introduced, such as commercial relations carried out in the digital environment and, consequently, the consumer relations they engender, might be considered one of the reasons behind this increase, since they have not yet been explicitly regulated by Brazilian law.

Consequently, e-commerce enterprises and suppliers carrying out commercial transactions over the Web frequently end up breaching consumer rights regulations. In Brazil it is difficult to pin down the rules governing the amount of information an e-commerce website must publish on its products and delivery deadlines, or refund procedures, given the uncertain status of these players in the consumer chain. This great legal insecurity related to online transactions leads enterprises to underrate the economic and innovative potential of this method of corporative action, at the expense not only of consumers but also their own. In fact, the lack of specific regulation governing commercial practice in the digital environment also creates various tension points for companies, such as the liability of content and hosting providers and the terms of use agreements.

Therefore, the inclusion of this issue in a broader review process, involving the actual CDC, suggests an inevitable integration between consumer protection regulation and consolidated e-commerce practice, which represents an increasingly greater share of the consumer market.

With regards to the Mercosur, the Brazilian Science and Technology minister, Aloizio Mercadante, announced in December that the southern bloc is drafting common e-commerce regulations[116], aiming at promoting free trade efficiency among its member States, not only in relation to transactions carried out across

[115] Data obtained at: <http://idgnow.uol.com.br/internet/2012/01/25/defensoria-publica-do-rio-notifica-sites-de-compras-coletivas-e-vendas-online/>. Accessed on 19.07.12.

[116] Information obtained from the article: <http://g1.globo.com/tecnologia/noticia/2011/12/mercosul-prepara-regulacao-comum-para-comercio-eletronico.html>. Accessed on 07.03.12.

physical borders, but also in the virtual environment, thus providing legal safeguards. Courses on e-commerce will be offered by the Mercosur Virtual School[117], a project of Mercosur Digital.[118] This project is a partnership between the Latin bloc and the European Union, aimed at promoting economic integration within the bloc through challenges imposed by the Information Society, reducing technological asymmetries and fostering common policies in information and communication technology, with e-commerce as one of the main focuses.

7.2 E-commerce regulation in 2011

A search for the terms "e-commerce" or "ecommerce" in the website of the House of Representatives[119] will reveal that five bills were submitted in 2011; in contrast, only one or two bills on this topic were submitted in each of the previous years since 1999. This shows a growing concern in 2011 in relation to e-commerce regulation, which is commensurate with the sector's expansion in the last two years.

Two of the bills require businesses selling products online to publish company information (company registration number [CNPJ], address and telephone of facilities), namely Bills no. 2,367/2011 and 1,232/2011. This is justified by arguing that, in many cases in which purchasing problems arise, the lack of company information makes it difficult for the consumer to seek redress, file a complaint at consumer protection agencies and take legal action, which requires the name or address of the corporation.

Bill no. 2,096/2011, on the other hand, "calls for including the obligatory publication of e-commerce product and service prices". This shows an additional concern with e-commerce practices regarding the information provided to consumers and its consistency with what is offered.

---

[117] By 2012, detailed information on the courses was already available at the Mercosur Virtual School website: <http://www.metaanalise.com.br/inteligenciademercado/index.php?option=com_content&view=article&id=6356:escola-virtual-do-mercosul-cursos-de-comercio-eletronico&catid=8:carreira&Itemid=358>. Accessed on 07.03.12.

[118] Available at: <http://www.mercosuldigital.org/>. Accessed on 07.03.12.

[119] Available at: <http://www.camara.gov.br/sileg/Prop_lista.asp?formulario=formPesquisaPorAssunto&Ass1=com%C3%A9rcio+eletr%C3%B4nico&co1=+OR+&Ass2=e-commerce&co2=+OR+&Ass32=ecommerce&Submit2=Pesquisar&sigla=&Numero=&Ano=&Autor=&Relator=&dtInicio=&dtFim=&Comissao=&Situacao=&OrgaoOrigem=todos>. Accessed on 07.03.12.

Two of the bills introduced refer specifically to regulating online group buying – Bill no. 1,933/2011 and Bill no. 1,232/2011, which are described in greater detail below.

7.3 Regulation of group buying in 2011

Online group buying is a new type of e-commerce that has expanded rapidly in the Brazilian market in the last two years – more than 2,000 group buying websites were created in Brazil in this period alone.[120] This evidence of its economical potential – i.e. for attractive, reasonably priced offers, thanks to the number of consumers drawn to the same offer – was accompanied by increasing complaints and potential violations of consumer rights. For instance, the number of complaints filed at the Procon of Rio de Janeiro increase seven-fold in 2011 (from 49 in 2010 to 353).[121]

The great number of complaints did not go unnoticed by the state of Rio de Janeiro's Legislative. On November 18, 2011, Rio de Janeiro pioneered group buying regulation introducing the Group Buying Bill, no. 1,062/2011, which "sets forth parameters for group buying of products and services through websites in the state of Rio de Janeiro".[122]

Also worthy of note, 2011, there was a federal bill on group buying submitted to the House of Representatives on May 4, Bill no. 1,232/2011[123], which aims at regulating group buying at a national level. The document of the federal bill is quite similar to the Rio de Janeiro bill, differing in that the former establishes a minimum period of six months for the purchased offer to be used, while the latter sets it at three months. Another difference is the requirement of the federal bill that websites be hosted in platforms belonging to companies with headquarters or branches in Brazilian territory, in order to facilitate communication between consumers and companies in case of post-sale or contract issues.

---

[120] Data obtained from: <http://www.tiinside.com.br/13/02/2012/rio-sai-na-frente-e-cria-lei-para-sites-de-compras-coletivas/ti/262358/news.aspx>. Accessed on 06.03.12.

[121] Data obtained from: <http://www.proteste.org.br/consumidor/rio-eeacute-pioneiro-em-lei-para-compra-coletiva-s566811.htm>. Accessed on 06.03.12.

[122] It is noteworthy that this Bill was approved and enacted on January 9, 2012 as Law no. 6,161/2012.

[123] Available at: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=500481>. Accessed on 06.03.12.

Furthermore, the Rio de Janeiro bill foresees that a breach in the buy-sell agreement will generate "obligations for the group buying company or the company responsible for offering the product or service" (article 7), but does not define such obligations; whereas the federal bill foresees joint liability for both companies for veracity of information and potential damages to consumers.

The sector responded that same year by launching a Code of Ethics aimed at setting forth rules for group buying businesses and reacting to the proposed bills. This is an initiative[124] by the Group Buying Committee of the Brazilian Chamber of Electronic Commerce, which comprises the sector's main enterprises accounting for 85 % of the industry's turnover. The code provides rules for good group buying practices, such as barring false offers and the manipulation of buying totals in order to influence users on the offer's success, as well as establishing clearer opt-in/out systems. Organizations that comply with the code will be awarded an excellence certification.

7.4 Tax war in e-commerce

On April 1, 2011, the National Council of Economic Policy – CONFAZ[125] – published ICMS (state tax on goods and services) Protocol no. 21[126], which aims at benefitting subscribing states with the right to collect tax on products "purchased from a company through remote selling".[127] However, not enough attention was paid to the consequences of this policy, which can influence prices and the quality of the service provided to consumers. It was an attempt by states to collect part of the taxes generated by the billions traded in online shopping.

---

[124] Available at: <http://www.camara-e.net/Compras-Coletivas/etica/codigo-de-etica-em-compras-coletivas.pdf>. Accessed on 19.07.12.

[125] According to article 155, paragraph 2, g of the CR, the complementary law must regulate how States and the Federal District will be allotted tax benefits, based on their deliberations. The Complementary Law that corresponds to this provision is law no. 24/75 substantiated by paragraph 8 of article 34 of the ADCT, which sets forth that ICMS exemptions and benefits must be determined by a covenant entered into and signed by the states and the Federal District. The body in charge of such covenants is CONFAZ, which is comprised by a representative from each state and one from the Federal District and one from the State.

[126] Available at: <http://www.fazenda.gov.br/confaz/confaz/protocolos/icms/2011/pt021_11.htm>. Accessed on 08.03.12.

[127] Quoted from the preamble of Protocol 21: "Regulates ICMS requirements in inter-state operations that deliver goods or assets to end customers, which are purchase remotely from the sending facility."

Sharing the proceeds of online sales has become more and more attractive, due to the easy and convenient transactions, the innovative and unique offers, which attract a diversified consumer base, and the possibility of offering lower prices afforded by expense cuts in many pricing components.

The rationale for this tax war in e-commerce lies on social changes and technological progress unforeseen by the current Constitution and, therefore, by the infra-constitutional regulations applied to consumer relations. The Federal Constitution rules that, when the recipient of the product is the end consumer (as in e-commerce), state tax on that product will be entirely collected by the state where the good was produced. In contrast, when the recipient is, for example, a retail business which will resell the product, the state where the business is established will collect part of the tax. This is one of the reasons for the low price of products sold online.

Given the high tax potential of e-commerce and the sector's dominance by states in the South and Southeast regions of Brazil, the remaining states started pressing for fiscal policy changes in order to adjust the collection of state tax on goods and services to the new market reality afforded by the Web. These states claim that, without the benefits of the CONFAZ Protocol, their local economies and regional development would be severely affected. They also claim that the ICMS is a tax on consumption and, consequently, should be jointly collected by the origin and destination states, as provided in the first clause of the Protocol.[128] These provisions would only relate to products purchased by distance selling through the Internet, telemarketing or showrooms.

The problem of this dispute among states is the possibility of double taxing of products – states such as Bahia have issued laws obligating consumers to pay an extra ICMS rate on delivery, preventing it from being withheld by the State Finance Department.[129] However, this surcharge is charged without the corresponding discount of this percentage from the ICMS incorporated in the price at the time of purchase. As states wage their tax war, consumers are the

[128] "First clause. Federative units undersigning this protocol agree to collect, subject to the terms herein, for the benefit of the federative unit of destination of the good or asset, part of the Tax on Goods and Services and on Interstate and Inter-municipal Transport and Communication Services Provided – ICMS – due on interstate operations in which the end customer purchases a good or asset remotely, through the Internet, telemarketing or showroom".

[129] Taken from the article: <http://economia.ig.com.br/estados+declaram+guerra+por+impostos+do+comercio+eletronico/n1238157416089.html>. Accessed on 08.03.12.

ones who stand to lose the most, either by being forced to pay more or by facing potential delivery issues.

The double taxing was criticized by institutions such as the Brazilian Institute for Consumer Protection (Idec) and the Brazilian Order of Attorneys (OAB), which filed a lawsuit challenging the constitutionality of the CONFAZ Protocol. In the lawsuit, the OAB claims that, although the Constitution provides state autonomy to regulate ICMS-related issues, this should not prevail over the norm specifying tax collection only by the state of origin when the recipient is the end consumer, to avoid double taxation. Consumer protection agencies have pointed out that this can greatly affect the development of the e-commerce sector, which has proved to be effective and interesting both to consumers and suppliers, besides being a market innovation, but which may suffer under the burden of excessive taxation.

8

Access, Infrastructure and Architecture

8.1 The National Broadband Plan

The so important access to the network is enabled by a seamless high speed connection, such as broadband. Broadband infrastructure of access to the Internet is one of the main tools to promote social and economic development, since it provides better quality Internet services and enables innovation on the network. When available in large scale, it meets the demands of its different users – i.e. government, private sector and citizens.

However, broadband connections are still restricted and not widespread across the national territory. In a population of 191.5 million Brazilians[130], at the start of 2011 there were only 16 fixed broadband connections and 28 mobile broadband connections.[131] Although these numbers are on the rise, there is still a demand for quick expansion of broadband connections; several countries have been

[130] Data from the Diagnostic Assessment of the IPEA on the Current Situation of Broadband in Brazil carried out by the Brazilian Telecommunications Association (Telebrasil). Available at: <http://www.telebrasil.org.br/pnbl_sinditelebrasil_teleco_situacao_banda_larga_no_brasil.pdf>. Accessed on 04.06.12.

[131] Data from the Technical/Consultancy Report Analysis of the Use of the 700 MHz spectrum, by the Brazilian Telecommunications Association (Telebrasil). Available at: <http://www.telebrasil.org.br/analise_de_utilizacao_do_espectro_parte1.pdf>. Accessed on 04.06.12.

implementing Plans to ensure this[132], which puts Brazil at a disadvantage if we fail to take any measures.

In view of the "existing serious inequalities in broadband access conditions in the country"[133], the government launched on May 05, 2010, an action Plan, namely the National Broadband Program (PNBL)[134], created by Decree 7,175/2010.[135] The goal of this plan is to enable access across the country by 2014, which was defined in principle as reaching 40 million households, from a starting point of only 11.9 million households with access to the broadband infrastructure. This figure, however, was been revised in the second document launched by the Ministry of Communications, namely the National Broadband Plan[136], which sets forth more detailed targets and includes details of the main executors of the Plan, as discussed later in this document.

Hence, the target of the PNBL was readjusted to 30 million fixed broadband access points and 60 million mobile broadband access points (urban and rural) by 2014, in addition to 100% broadband reach in Government bodies and 10-fold increase in the minimum speed of fixed broadband services (quality of service criterion). The estimated investment required to reach these targets is of BRL 49 billion (private and public funding through credit lines, such as the BNDES').

Although the aim of this document is not to set specific figures for adequate broadband speed (its aim is simply to ensure that the broadband infrastructure

---

[132] "Due to their potential to boost the economy, national broadband expansion plans have been implemented by several countries in their economy recovery packages after the 2008 world crisis [8]. The U.S., Great Britain, Canada, Germany, Portugal, Italy and Finland have all included specific measures for this purpose. Different initiatives in Australia, France, Ireland, Japan, Singapore and South Korea have also foreseen broadband infrastructure improvements and expansion. An example of Latin American country that has a related action plan is Chile; their plan, among other initiatives, foresees coverage targets for broadband connections [10]". PNBL, page 23.

[133] Letter published during the launch of the PNBL. Available at: <http://campanhabandalarga.org.br/index.php/2011/01/20/40/>. Accessed on 11.07.12.

[134] Available at: <http://www.google.com.br/url?sa=t&rct=j&q=plano%20nacional%20de%20banda%20larga%20download&source=web&cd=3&ved=0CGYQFjAC&url=http%3A%2F%2Fwww.governoeletronico.gov.br%2Fanexos%2Fplano-nacional-de-banda-larga%2Fdownload&ei=QHD0T4_1ElGg8QSLiPnqBg&usg=AFQjCNHK78IA39qh-TjnwT92Ngk9yM-IBQ>. Accessed on 04.07.12.

[135] Available at: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Decreto/D7175.htm>. Accessed on 13.07.12.

[136] Available at: <http://www.google.com.br/url?sa=t&rct=j&q=plano%20nacional%20de%20banda%20larga%20pdf&source=web&cd=3&ved=0CFsQFjAC&url=http%3A%2F%2Fwww.governoeletronico.gov.br%2Fanexos%2Fplano-nacional-de-banda-larga%2Fdownload&ei=TpIAUKKKOoHb6wH596SNBw&usg=AFQjCNHK78IA39qh-TjnwT92Ngk9yM-IBQ>. Accessed on 13.07.12.

available meets the needs of consumers and service providers), one of the main targets of the National Broadband Plan was originally to provide affordable services packages with speeds from 512 to 784 Kbps for BRL 35.00. With the Dilma Rousseff administration's intervention, this speed was increased to 1 Mbps – i.e. at this rate it takes two hours and forty minutes to download a 1.2 GB file.[137]

8.1.1 Agreements

The affordable broadband service packages foreseen by the PNBL were created initially by Agreements between the Ministry of Communications and Anatel and the main fixed telephony concessionaries (Telefônica, Oi, Companhia de Telecomunicações do Brasil Central – CTBC and Sercomtel) on June 30, 2011.[138] Since these plans were to be implemented by the private sector – i.e. the Government was prevented from imposing prices or service level targets -, affordable plans were created as part of the 5-year review of concession agreements and of the General Plan for Universalization targets.[139] They also foresee that companies must charge BRL 29.90 in areas of ICMS exemption.

These Agreements, however, have been the target of by severe criticism.[140] The first criticism is to the fact that these agreements foresee private management of broadband services, which would prevent the government from directly protecting the interests of the population. In other words, the Government

[137] Available at: <http://g1.globo.com/tecnologia/noticia/2011/06/entenda-o-plano-nacional-de-banda-larga.html>. Accessed on 13.07.12.

[138] The Ministry of Communications provides the full content of these agreements at: <http://www.mc.gov.br/acoes-e-programas/programa-nacional-de-banda-larga-pnbl/252-temas/programa-nacional-de-banda-larga-pnbl/23723-termos-de-compromisso>. Accessed on 13.07.12.

[139] Also from June 30, 2011, the PGMU sets forth that the "National Telecommunications Agency (Anatel) must implement, by October 31, 2011, the necessary regulatory measures to create quality standards for telecommunications services to support access to broadband Internet connections -i.e. defining, among others, minimum and medium effective connection speeds and service availability parameters, as well as advertising and transparency rules to enable assessing perceived quality by users." Available at: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Decreto/D7512.htm>. Accessed on 13.07.12.

[140] An example is the "Banda Larga é um Direito Seu!" (You are entitled to broadband!) Campaign, which gathers a series of organizations that defend cheap and good quality Internet access to all. As a means of taking action, they prepared a Manifest, which may be signed by anyone, claiming for broadband to be dealt with as a basic service, to be provided by the government, thus ensuring equality among providers and sustainable introduction of new agents. The Manifest may be viewed at the link below: <http://campanhabandalarga.org.br/index.php/manifesto/>. Accessed on 13.07.12.

would be subject to the contracted terms, when, in fact, it should play an active part as economic agent and provider of this service; this would be necessary if it were to reach the target of taking the broadband infrastructure country wide.

There would be a problem regarding the download limit imposed by affordable plans, since exceeding it would allow concessionaries to reduce the contracted Internet speed (without any prejudice to basic applications), thus limiting full use of the Internet by consumers. Such measure would seem like an attempt by concessionaries to make these plans less attractive to consumers – in addition to reflecting poor quality standards, because the 1 GB limit would be easily reached given that online applications, cloud hosting and video streaming have posed increasing demands on bandwidth. According to an Idec study, the International Union of Telecommunications claims that broadband quality should be at least 1.5 Mbps download speed.[141] Furthermore, the consumer who contracts these plans will also have very limited upload capacity: of up to 128 Kbps, which corresponds to just over the twice the speed of a dial-up connection.[142]

Moreover, the agreements oblige concessionaries to operate exclusively in the "main centers of municipalities", which does not include the whole of urban areas or rural areas. This is in line with the general universalization targets set forth by the National Broadband Plan, which foresees that the broadband Internet connection infrastructure should cover both urban and rural areas, reaching all municipalities in the country with more than 100 thousand inhabitants.[143]

---

[141] Available at: <http://www.idec.org.br/em-acao/revista/abertura-de-contas/materia/lenta-cara-e-para-poucos-ii-a-missao/pagina/109>. Accessed on 16.07.12.

[142] The maximum speed of dial-up Internet connections is 56.6 Kbps. Data from Wikipedia: <http://pt.wikipedia.org/wiki/Linha_discada>. Accessed on 16.07.12.

[143] Page 17 of the PNBL.

One of the most worrying issues was that the Agreements allowed sale of affordable plans with public switched landline service plans.[144] Allegedly, this practice would involve a combined sale of the broadband plan and the landline service, which is expressly forbidden by the Consumer Protection Code.[145]

Hence, critics of the program claim that implementing these terms is proof of the lack of a consolidated action plan across the Federal Government; not to mention the fact that it would promote large scale expansion of a poor quality service, which has been the target of constant customer dissatisfaction due to excessive defects.[146] According to Procon's Registry of Substantiated Complaints in 2011[147], "poor broadband Internet connection services have also been targeted by complaints, due to frequent service outages and speeds lower than the contracted ones. There have also been complaints related to the lack of information on Internet access packages for international roaming" (page 13).

The telecoms Telefônica and Oi, which signed Agreements in connection with the PNBL, ranked very badly according to the Procon report – i.e. they ranked 6th and 7th, respectively, among the 50 companies with the most complaints in 2011, in addition to featuring among the 5 basic services companies most complained about (only below Tim). In regards to this survey, it is noteworthy that Procon also acknowledges the potential disadvantages for customers in purchasing a combined plan with landline and broadband connection services

[144] For example, in the Agreement with the CTBC (available at: <http://www.mc.gov.br/acoes-e-programas/programa-nacional-de-banda-larga-pnbl/252-temas/programa-nacional-de-banda-larga-pnbl/23723-termos-de-compromisso>), the following provisions have been included: "§3 The case foreseen in paragraph 2 does not exempt ALGAR TELECOM from making their Retail Offer available through the SCM or by using technology of equivalent technical quality, as per the schedule foreseen in ANNEX I, which may be offered jointly with the public switched telephony service (PSTS) available at the locality, as per paragraph 4 of this Clause.
§4 Notwithstanding the provisions in paragraph 3, ALGAR TELECOM must provide consumers with the option to contract the Retail Offer, for the price specified in the header herein, jointly with the Basic PSTN Plan, homologated under the terms of Annex III of the Concession Agreement. Alternatively, it may be combined with at least one Alternative PSTN Plan, which must cost up to BRL 30.00 (thirty Brazilian Reais), with taxes, notwithstanding charges for (i) PSTN routed traffic exceeding the plan; (ii) provision of utilities or commodities (PUCs); and/or (iii) other services."

[145] Article 39. The following, among other abusive practices, are forbidden to products or service providers: I – conditioning the supply of a product or service to another product or service, as well as to unjustified amount limits;

[146] *Sinais preocupantes: o PNBL em momento crítico* (Worrying Signs: a critical time for the PNBL) , Banda Larga é um Direito Seu! Campaign. Available at: <http://campanhabandalarga.org.br/index.php/2011/06/13/sinais-preocupantes-o-pnbl-em-momento-critico/>. Accessed on 16.07.12.

[147] Available at: <http://www.procon.sp.gov.br/pdf/acs_ranking_2011.pdf>. Accessed on 16.07.12.

(permitted by the Agreements), drawing Anatel's attention to the need to regulate this practice.[148]

8.1.2 PNBL Management

According to Decree 7,175/2010, the main manager of the National Broadband Plan would be the state company Telecomunicações Brasileiras S.A. (Telebrás), which would work with the Digital Inclusion Program Steering Committee (CGPID), Anatel and telecoms concessionaries. Telebrás would be responsible for implementing the private communications network for the federal government, for providing support to broadband Internet connection public policies for universities, research centers, schools, hospitals, service centers, community telecenters and other centers of public interest, in addition to providing the telecommunications services support infrastructure and networks for private companies, states, the Federal District, municipalities and non-profit organizations. Hence, the government would head implementation of the Plan and the private sector would have a supporting role – i.e. would be responsible, for example, for providing broadband services directly to end users. What's more Telebrás would only replace infrastructure in places where the services available were below adequate.

This role division between the public and the private sector, however, changed during 2011 when the implementation of the PNBL was accelerated by the Ministry of Communications (which had changed hands again when the Lula administration was replaced by president Dilma's Government).[149] The role

---

[148] "Offering packages with comparatively better value pricing and conditions than contracting services alone inhibits single-service contracting. The apparently advantageous services packages, however, conceal issues that may be faced later on by customers.
Information is usually unclear at the time when services are purchased from one of the companies involved – i.e. the different service providers, specific regulatory standards for each service and special conditions for the package. When a customer has issues, is unhappy with the service or wishes to withdraw from one or more services, he/she goes through a process of being "pushed around" by these companies. Moreover, he/she is notified of fines payable for breaching the loyalty clause (paid TV and mobile telephony) and of the revised pricing for the service that will remain active.
Procon-SP stresses the need for regulation of converging services by the National Telecommunications Agency (Anatel), as there are different rules for the different services included in these packages, such as loyalty clauses, which are allowed for some services and forbidden for others." Page 12 of the Substantiated Complaints Registry for 2011, Procon. Available at: <http://www.procon.sp.gov.br/pdf/acs_ranking_2011.pdf>. Accessed on 16.07.12.

[149] On January 01, 2011, minister Paulo Bernardo Silva took office in the Ministry of Communications, and former minister José Artur Filardi, who had taken over on March 31, 2010, from the former minister Hélio Costa, one of the creators the PNBL, resigned.

of telecoms concessionaries became increasingly prominent in the PNBL, thus restricting the role of Telebrás, which focused on the development of backhauls.[150] Even before the Agreements were signed, the Ministry of Communications already showed signs that the implementation of the PNBL would be supported by telecoms companies. This was stated in an explanatory note from the Ministry to the Sao Paulo Stock Exchange (Bovespa) and the Securities Commission (CVM): "the Ministry intends to review the market role of Telebrás aiming to reduce the company's isolated projects and to focus its combined efforts with the private sector towards the expansion of the country's networks and wholesale trading".[151]

The National Broadband Plan itself attests of this understanding, as it states that one of its principles "is to foster competition in the private sector for investments on broadband infrastructure, allowing the State to take on a supporting role (...)".[152] In addition to that, a series of political initiatives shows how Telebrás is moving away from its original role in the PNBL. One such initiative was Dilma's Government's axing of funds – while the Lula Administration foresaw an initial investment of BRL 1 billion to Telebrás by the end of 2011, with potential additional BRL 400 million, "the initial BRL 600 million was reduced by the current administration to BRL 316 million, with further reductions that will prevent reaching the PNBL's target for 2011".[153]

There have also been suggestions that the dismissal of the president of Telebrás and creator of the PNBL, Rogério Santanna (on May 31, 2011), and of the Secretary of Telecommunications, Nelson Fujimoto, evidence an intention

---

[150] "Backhauls are the links within the large networks set up in municipalities, from which the signal is distributed to the networks that provide broadband connections to households". Banda Larga é um Direito Seu! website, *Entidades criticam negociação do governo com as Teles* (Entities criticize Government negotiations with Telecoms), available at: <http://campanhabandalarga.org.br/index.php/2011/04/25/entidades-criticam-negociacao-do-governo-com-as-teles/>. Accessed on June 13, 2012.
According to the National Broadband Plan, "In regards to limitations to the expansion of broadband infrastructure availability, Brazil has been working towards overcoming one of the main limiting factors to broadband coverage expansion, namely expanding the backhaul to more locations. (...) It is worth stressing the importance of non-discriminatory availability of the backhaul to access nodes" (page 13).

[151] Related to Official Note 561/2011/SE-MC, available at: <http://www.bmfbovespa.com.br/agencia/corpo.asp?origem=exibir&id=18201105030168&manchete=TELEBRAS%20(TELB)%20-%20ESCLARECIMENTOS>. Accessed on 16.07.12.

[152] Page 11 of the PNBL.

[153] *CUT defends strengthening of Telebrás*, Banda Larga é um direito seu!, available at: <http://campanhabandalarga.org.br/index.php/2011/06/06/cut-defende-fortalecimento-da-telebras/>. Accessed on 16.07.12.

to shrink Telebrás and its role as manager of the Plan. Santanna had criticized the government, claiming that it was succumbing to the interests of telecoms concessionaries, and that there was no need for such close proximity with the private sector, as the network targeted by Telebrás already exists – i.e. as a product of agreements between Telebrás, Petrobras and Eletrobrás, which will be discussed later – and would become profitable in five years. Hence, the network would only have to be strengthened (economically and professionally) and expanded, but these plans would be unfeasible with the funding cuts to the state company.

On the other hand, the current minister of Communications, Paulo Bernardo, claims that this negotiation with telecoms companies was necessary, as the investment foreseen to reach the PNBL targets was of BRL 7 billion and president Dilma Rousseff only authorized public funding of BRL 1 billion a year – that is, BRL 4 billion in total (if the 2011 budget is maintained). According to the minister, reaching the plan's targets is critical, regardless of whether this is carried out through public or private funding, and without making it into a competition between Telebrás and telecoms companies.[154] Santanna, on the other hand, believes that the monopolies of the main telecoms companies hinder the competition. As a result, customers living in areas with no broadband service available suffer, despite representing a large share of the population, because they are at the mercy of the interests of companies and the Agreements executed with them (which, as discussed, only oblige companies to cover the main areas of municipalities).

The aforementioned evidences one of the main criticisms against the PNBL and the privatization of access to the broadband infrastructure: there is no requirement for the services to be universalized. According to the Banda Larga é um Direito Seu! campaign, broadband access should be managed as a basic right and essential service; this would ensure that it would be managed by the government and, therefore, have all the features of this type of regimen, such as universalization, pricing control and return of related assets to the Nation's treasury.

Such regimen would also enable using funds from the FUST (Telecommunications Services Universalization Fund) to implement the PNBL, which cannot be done under a private regimen. The FUST raises BRL 600 million annually, from taxes

[154] Data from the Observatory of the Right to Communication. Available at: <http://www.direitoacomunicacao.org.br/content.php?option=com_content&task=view&id=7924>. Accessed on 16.07.12.

on the gross operating revenue of all companies in this industry, according to the PNBL (page 127). Currently, the law that governs the use of these funds is under revision[155] and, if approved by the Congress, shall enable their use for any investments on telecommunications services, provided both publicly and privately, including access services to the broadband infrastructure. The rationale for the bill is that the Fund has already raised approximately BRL 5 billion, which haven't been used for the designated purposes.

Despite all of the efforts to depose Telebrás as PNBL manager, it implemented a series of initiatives in 2011 to complete the Plan. For example, it negotiated with Petrobrás[156] and Eletrobrás[157] the right to use their fiber optics networks, without which it would be impossible to reach the expansion targets foreseen – this agreement was later objected by a lawsuit filed by the telecommunications companies at the end of November.[158] Furthermore, it entered into agreements with the companies Claro and Tim, which launched affordable broadband plans.[159] In November, in partnership with the RNP (National Research and Education Network), it launched a pilot project to integrate federal universities and technology institutes with the national academic network at high speed[160], which is to be implemented in the states of Tocantins and Goiás by expanding the backhaul of universities.

---

[155] The Bill for the revision of the Law governing the use of FUST funds is the Senate Bill no. 103, from 2007. Available at: <http://www6.senado.gov.br/mate-pdf/9415.pdf>. Accessed on 16.07.12.

[156] About the agreement to use the fiber optics network with Petrobrás: <http://www.brasil.gov.br/noticias/arquivos/2011/05/19/petrobras-cede-utilizacao-de-fibras-opticas-para-programa-nacional-de-banda-larga>. Accessed on 16.07.12.

[157] About the agreement to use the fiber optics network with Eletrobrás: <http://insight-laboratoriodeideias.blogspot.com.br/2011/07/telebras-e-eletrobras-juntas-para.html>. Accessed on 16.07.12.

[158] Teles vão à Justiça para que Telebras abra contratos firmados com Eletrobrás e Petrobras ("Telecom companies go to Court to force Telebras to open its agreements with Eletrobrás and Petrobras"), Convergência Digital. Available at: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=28479&sid=14>. Accessed on 16.07.12.

[159] About Claro: <http://oglobo.globo.com/tecnologia/claro-adere-ao-programa-de-banda-larga-do-governo-oferece-servico-r-2990-2868224>. About Tim: <http://info.abril.com.br/noticias/tecnologia-pessoal/com-tim-pnbl-tera-web-movel-por-35-reais-13072011-30.shl>. Accessed on 16.07.12.

[160] About the pilot project between Telebrás and the RNP: <http://portal.rnp.br/web/rnp/imprensa/-/rutelistaconteudo/6Cal/articleId/608535/groupId/489970/templateId/TPL-IMPRENSA-RNP/isPrintable/true>. Accessed on 16.07.12.

8.2 Quality Management Regulation for Fixed and Mobile Internet Services

In July 2010, Anatel launched a public enquiry[161] to design a Quality Management Regulation for Personal Mobile Services (RGQ-SMP), aiming to update the General Targets and Quality Plan (PGMQ-SMP)[162] in force at the time and to add new quality indicators to be met by mobile telephony services providers.

In August 2011, the agency adopted the same procedure[163] for Multimedia Communications (RGQ-SCM). As a result of these enquiries, the agency approved to Quality Regulations in 2011, namely the RGQ-SCM[164] and the RGQ-SMP.[165]

The fact that Anatel implemented Quality Management Regulations is relevant because they set forth quality standards to be met by services providers. Failure to comply with the Agency's quality standards, compulsory from November 2012[166], may impose sanctions on providers.[167]

In regards to regulation of the Multimedia Communications Service[168] – i.e. telecommunications service that supports broadband access to the Internet -, Anatel only set forth goals for providers with more than fifty thousand subscribers and for three types of indicators: Subscriber Reaction Indicators, Network Indicators and Customer Services Indicators.

---

[161] Public Enquiry no. 27/2010.

[162] Anatel resolution no. 317 from September 27, 2002.

[163] Public Enquiry no. 46/2011.

[164] Anatel Resolution no. 574, from October 28, 2011. Available at: <http://www.in.gov.br/visualiza/index.jsp?data=31/10/2011&jornal=1&pagina=91&totalArquivos=160>. Accessed on 29.02.12.

[165] Anatel Resolution no. 575, from October 28, 2011. Available at: <http://www.anatel.gov.br/Portal/exibirPortalRedireciona.do?codigoDocumento=245894>. Accessed on 20.07.12.

[166] According to article 46 of the Resolution, the targets become compulsory 13 (thirteen) months after the regulation has been approved.

[167] It is noteworthy that telecommunications services are a frequent source of customer complaints. According to the Ministry of Justice's Department for Consumer Protection and Defence, in 2011, telecommunications services accounted for 22.90% of the total customer complaints made to PROCON units, which are part of the SINDEC (National Information System for Consumer Protection).

[168] "The Multimedia Communication Service is a fixed telecommunications service of public interest. It is a private service provided nationally and internationally, which enables multimedia information transfer, sending and receipt, via any means, to members within an area where the service is provided." – transcribed from the definition in Article 3 of Resolution 272, from August 09, 2001.

For subscriber reaction indicators, Anatel set forth that SCM providers must bring down the number of complaints received through their service channels to a proportion of 6% of the total number of subscribers, from November 2012. From November 2014, the proportion of complaints must be reduced to 2% of the total number of subscribers. Similarly, Anatel set forth subscriber reaction indicators related to the number of complaints reopen.

The biggest innovation of the regulation was related to SCM providers' Network Indicators.

See below a few Network Indicators approved by the Agency:[169]

- Instant Speed: The speed measured at each measurement made by the software. Its result must not be below 20% of the maximum speed contracted by the Subscriber, both for downloading and uploading, in 95% of the measurements. The 20% target shall be in force in the first twelve month, from the effective date of the Regulation. In the next twelve months after that it'll increase to 30% and from then on to 40%.
- Average Speed: It is the result of the average of all measurements taken during the month in the provider's network. The initial target is 60% for the first twelve months. In the next twelve months after that it'll increase to 70% and from then on to 80%.
- Bidirectional Latency: Time it takes a data package to travel the network from a particular point to its final destination and back. The target for 95% of the measurements is of a maximum of 80 milliseconds for land connections and 900 milliseconds for satellite connections.

Equivalent network indicators have been approved for mobile telephony providers' data connections, according to Resolution no. 575/2011, which approved the RGQ-SMP.

Through Quality Management Regulations, Anatel also approved Customer Service Indicators for services provided through companies' Call Centers (CC) for service implementation times and problem solving, among other measurements.

[169] As published by Anatel on October 31, 2011. Available at: <http://www.anatel.gov.br/Portal/exibirPortalNoticias.do?acao=carregaNoticia&codigo=24110>. Accessed on 29.02.12.

During public enquiry periods, the agency received in excess of 300 contributions to the RGQ-SMP proposal and more than 700 contributions to the RGQ-SCM proposal.

International experiences, such as that of the British regulator that created the voluntary code of best practices[170] and the regulation by the Indian regulatory body (TRAI)[171] have substantiated the design of the regulatory proposal for Network Indicators, as well as a study carried out by INMETRO in partnership with the Brazilian Internet Steering Committee and Anatel itself.[172]

8.3 Domain names

All networked computers have an exclusive number referred to as "IP address", which enables locating them on the network and enables communications between terminals. In order to simplify these communications, a Domain Names System (DNS) was created to replace numbers by names. The Internet as we know it and use it today is based on domain names, which are on website addresses comprised of letters, words, sentences, individual names, company names and even brands. We can say that no user today remembers to access a website through number combinations.

Domain names play a much more prominent role than just enabling Internet users to access websites. Currently, the main efforts towards controlling users' conduct online are increasingly based on using domain names as an essential resource to identify users. The French government's initiative to oblige Internet access providers to block access to domain names is an example of this. On December 30, 2011, the French government edited a decree that obliged access providers to block online gaming websites that were not registered with the French gaming regulator ARJEL. Another good example of the relevance of domain names, which also took place in the past in France, was the use of such names in the presidential war between parties. The candidate for the French Socialist Party, François Hollande, whose motto was *Le changement, c'est*

---

[170] Available at: <http://stakeholders.ofcom.org.uk/telecoms/codes-of-practice/broadband-speeds-cop/voluntary-codes-of-practice/>. Accessed on 29.02.12.

[171] Available at: <http://www.dot.gov.in/Acts/legislation/6oct2006.pdf>. Accessed on 29.02.12.

[172] Available at: <http://www.inmetro.gov.br/consumidor/produtos/banda-larga.pdf>. Accessed on 29.02.12.

maintenant (now is the time for change, in French) launched his newspaper, *Libération*. On the following day, anyone who accessed the website www.lechangementcestmaintenant.fr would find a parody of the candidate's newspaper, *L'Hibernation* (hibernation, in French), and of his motto *Le reniement, c'est maintenant* (now is the time for denial, in French). The owner of the referred domain name registry was UMP, a rival party of the SP. When enquired about it, one of the members of the UMP's board alleged that François Hollande and his team failed to protect the candidate online.

Hence, the relevant role played by domain names is evidenced in several areas that reflect everyday situations of the non-digital world – i.e. whether in corporate operations or in the political battle between presidential candidates.

8.3.1 Proposals for regulating the topic in Brazil

Among the Bills (PL) under assessment by the National Congress, there are two proposals for domain names regulation in Brazil. The eldest proposal is an initiative by senator José Sarney, namely PL 256, from 2003. It focuses more on legal than technical aspects of domain names registration, setting forth requirements and conditions for registration. The second bill, from 2011, was written by Representative Claudio Cajado, whose main concern is to solve business issues related to domain names, particularly conflicts related to brands and corporate names; thus, preventing chaos and abuse of the "first come-first serve" principle that governs the domain names system.

BILLS ON DOMAIN NAMES REGISTRATION IN BRAZIL AND RESOLUTION NO. 8/2008 CGI.BR

	PL 835/2011	PL 256/2003	Resolution 8/2008
Definition	No definition	A domain name is regarded as a set of characters that identifies an address in the computer network, the Internet.	Top-Level Domains (TLD) are domains created under the .br ccTLD, which allow registration of sub domains according to the rules set forth in this Resolution.
Characteristics of the owner of the registration	Individuals or companies legally represented or established in Brazil, with a valid tax payer registration number (CPF) or company registration number (CNPJ).	Any individual or publicly or privately held company that meets the requirements set forth in this Law. Foreign individuals or companies who are not domiciled or headquartered in Brazil must appoint a proxy holder domiciled in the Country, with specific powers	Only entities operating legally in the Country, independent professionals and individuals are allowed to register a domain name, as per the provisions of this Resolution. Foreign companies may be allowed temporary registration, if they meet the requirements set forth in article 6 of this Resolution.
Registration restrictions	Expressions cannot be used for domain name registration under the .br categories, if they are contrary to moral and good conduct, offensive to the honor or image of people, or if they violate freedom of conscience, belief, religion or ideas and feelings worthy of respect and veneration, and individual names for which there are homonyms, except for the first applicant.	I – words or expressions that are vulgar or offensive to principles of moral and good conduct, to people's dignity, as well as that promote crime or discrimination against race, gender, color or beliefs; II – words or expressions that reproduce or copy, in full or in part, albeit with additions, a registered domain name, or one of the cases foresee in article 7, which could induce third-party error; III – names deemed by the registrar as damaging to the convenience, security and reliability of information traffic on the Internet.	The applicant has to agree not to choose any names in breach of the legislation in force, that may induce third-party error, violate third-party rights or represent pre-defined concepts of the Internet, that include vulgar or abusive words, that represent acronyms of states or ministries or other restrictions that may be set forth at the CGI.br's discretion.

BILLS ON DOMAIN NAMES REGISTRATION IN BRAZIL AND RESOLUTION NO. 8/2008 CGI.BR (CONTINUATION)

	PL 835/2011	PL 256/2003	Resolution 8/2008
Requirements	Is not easily mistaken by: I – brand registered with the National Institute of Intellectual Property not owned by the applicant; II – name of a facility, corporate name, civil name, family name, notoriously known pseudonym or nickname, individual or group artistic name, name of protected intellectual work or other domain name not owned by the applicant for which the latter has not obtained consent, copyrights and inheritance or succession rights; III – business names governed by domestic or international law, except when the applicant is a legitimate representative of the legal person; IV – official or officially acknowledged name, award or symbol of sporting, artistic, cultural, social, political, economic or technical event, except when the applicant is the promoter of the event; V – renowned brand in its industry, under the terms of the Paris Convention for the Protection of Industrial Property, even if not yet deposited or registered in Brazil.	I – no previous record of the name under the same top-level domain; II – not restricted under the terms of article 6 of this Law; III – proof of ownership or legitimate interest.	The most distinctive part of a domain name chosen for registration under a specific TLD, must: I. Have at least 2 (two) and a maximum of 26 (twenty six) characters; II. Be a combination of letters and numbers [a-z; 0-9], hyphen [-] and the following characters [à, á, â, ã, é, ê, í, ó, ô, õ, ú, ü, ç]; III. Not contain only numbers and not begin with a hyphen; IV. The domain chosen by the applicant must not configure a restricted name. Restricted names are those described in the single paragraph of article 1 of this Resolution.

BILLS ON DOMAIN NAMES REGISTRATION IN BRAZIL AND RESOLUTION NO. 8/2008 CGI.BR (CONTINUATION)

	PL 835/2011	PL 256/2003	Resolution 8/2008
Cancellation of registration	Not foreseen	I – express waiver by holder; II – expiration; III – void registration; IV – no longer meets holder or legitimate interest requirements, as per article 7; V – court order.	I. Express waiver by the holder, through relevant documents required by the NIC.br; II. Default on domain maintenance charges within the terms set by the NIC.br; III. Court order; IV. Proven irregularities in the registry data for the entity, described under article 4, subsection I, paragraphs 1 and 2, following proven failure to solve such irregularities in a timely manner upon the NIC.br's request; V. Breach of the agreement outlined in subsection IV of article 6 of this Resolution.

8.3.2 The International Debate

From January 12, 2012, website extensions are no longer limited to country acronyms and the traditional .com, .gov, .net and others. The Internet Corporation for Assigned Names and Numbers (ICANN), in charge of overseeing domain names on the Internet, has approved expanding potential Internet address extensions. The announcement was made at the start of the 41st meeting of the organization, which ended on June 24, in Singapore.

The measure was the main topic of the meeting. Main companies are expected to be the first to register new domain names for their brands. The new registration fee shall be of USD 185 thousand, and the high cost is viewed by the ICANN as a limiting factor to fraudulent registrations. It was very common on the Internet at first for people who were not at all related to a brand to register its domain name. Their motivation was to be able to sell the domain to the brand's rightful

owners. This was referred to as the new gold race of the digital era. In 1999, ICANN and OMPI prepared a Uniform Policy for domain names that also has provisions for conflict resolution.

The high cost of the fees charged is causing tension between stakeholders and fostering extensive debates and interpretation of ICANN's real agenda. Many believe that, in addition to reducing fraudulent registrations, the high fees will also be prohibitive for small and medium companies; thus, creating a hierarchy of domain names, which contradicts practices and expectations for the Internet. Another recurrent comment is that this measure enables ICANN and registrars to practically "print money": the race to register key suffixes for the brand positioning of several companies, as well as the necessary protections against ill-use by third parties, uncovers a new market created exclusively by this measure.

The launch of new domains is just one more stage in a long process of perfecting how content is addressed on the Internet. We'll now need to verify the authenticity of applications and resolve a series of conflicts, which will inevitably arise, particularly in regards to intellectual property.

Another controversial aspect of the new regulation is that it allows the registration of a domain that may affect morality and public order to be contested. The cultural diversity between countries is an obstacle to setting uniform parameters – e.g. the diversity of alphabets in view of the predominance of the western alphabet -, and this measure could potentially stir conflicts involving expressions that may be forbidden in a country, but not in others.

8.4 The Role of the NIC.br/CGI.br in technical solutions implementation for the Brazilian Internet

The Brazilian Internet Steering Committee (CGI.br), mainly through its executive arm, the Brazilian Network Information Center (NIC.br), closely monitors the technological development of the Internet. It has implemented several initiatives to monitor and influence how technologies are adopted and used by Brazilian networks, aiming to contribute to ensuring that the Internet develops under the same principles that have made it what it is today – i.e. an open network that fosters innovation and is increasingly universal.

From a technological standpoint, the Internet is a global network that interconnects computers, tablets, mobile phones and endless other devices.

In fact, as indicated by its very name, it comprises interconnections between several somewhat independent networks. These networks are managed by different institutions, which have different purposes and use devices from several manufacturers. Hence, the Internet can only exist because all of its participants agree to abide by a common set of technological standards, created openly and collaboratively and approved by approximate consensus by the ETF (Internet Engineering Task Force). There are literally thousands of standards that determine how every feature, service and application must work on the network.

The technologies used on the Internet are not neutral. The way they are created and used may steer the network as much as its policies – i.e. in the most traditional sense of the term already extensively used in this publication. The decentralization of the operations governing the Internet, which converge technologically, is also an important aspect for policy-making.

Few areas of the technological base of the Internet require centralized control – e.g. IP addresses, which identify every device, for being unique or the domain names system, due to the need for a starting point for Internet searches. These areas are key to debates on Internet technologies and policies, as centralization requires organization and role and resource allocation. This where the RIRs *(Regional Internet Registers*) and the ICANN *(Internet Corporation for Assigned Names and Numbers)* come in; they manage IP numbers and domain names, respectively, on the network.

Furthermore, several factors intrinsically related to technology or to how it is used potentially influence policies. Below we will discuss in more detail the main initiatives of both entities in charge of providing technical solutions to certain issues faced on the Internet – the CGI.br and the NIC.br.

8.4.1 IPv4 and IPv6 exhaustion

IP is the most paramount technological foundation of the network, i.e. the protocol after which it is named – Internet. It is worth remembering that the Internet is built on the traditional telecommunications infrastructure, which is the same infrastructure used for telephony, radio and TV services. Nonetheless, it is usually much more flexible and cheaper than the others, as it uses resources much more effectively. In other words, instead of using circuit communication, which requires reserving the resources needed for the communication between the sender and the receiver in advance, the Internet uses packet

switching; this technique divides the information into small blocks that can be sent independently across the network to their final destination. Packet communication ensures both effective sharing of telecommunications resources and building extremely resilient networks, which creates several different paths between any two points.

IP addresses are specifically what set the Internet apart from other telecommunications services. The Internet Protocol is, therefore, identifies each device connected to the network through a number that we call address, in addition to encapsulating and aggregating information to all data exchanged through it enabling them to reach their destination. The IP uses several different types of telecommunications networks, creating a standardized layer upon which all other Internet protocols and services work.

IPv6 is the most recent version of the IP. It has to be implemented quickly, because its former version, the IPv4, can no longer support network expansion – i.e. there are no more addresses available.

The NIC.br has been working to support and foster the implementation of the IPv6 in Brazil for several years. In December 2007, it started allocating new addresses. In 2008, a series of promotion actions was launched, including technical lectures in events and universities, building a related website in Portuguese[173], creating and making educational materials available, as well as an e-learning course on the subject, setting up an educational lab and creating a free theoretical and practical course for Internet and other autonomous systems providers' employees, providing free IPv6 traffic, creating a validation tool for IPv6 websites and, finally, carrying out surveys on the quality of the IPv6 infrastructure on the Internet, among others. In 2011 alone, there were 200,000 accesses to the website created by the NIC.br, and approximately 700 technicians were trained in 21 practical courses provided throughout the year in all regions of the country. There were also two main technical events on IPv6 for case presentations.

In addition to its technical actions, which focused on raising awareness and training technicians to plan, implement and operate the IPv6 on the Internet, in 2011, the NIC.br also carried out several management activities. Meetings

[173] The website address is <www.ipv6.br>. Accessed on 18.07.12.

were held between the NIC.br and several stakeholders, particularly telecoms operators, access providers and Internet content providers and, as a result, a large operational test of the protocol was planned for the start of 2012: the IPv8 Week. Moreover, a timetable was outlined to steer protocol implementation in the country, according to which telecoms operators and providers must enable traffic through their corporate products by mid-2012 and must begin to set up protocol support for domestic users by the start of 2013. On this date also, all Brazilian websites are also expected to support the protocol.

Transitioning to IPv6 is paramount for the network and there are several risks involved. One of the main risks is related to the use of IPv4 support technologies, which are well known and have been used since the mid-90s – the main such technology is the NAT. However, the capacity for using them without prejudice to network operation and to its basic principles, such as peer-to-peer connectivity and neutrality, has already been exhausted. Use of the NAT by Internet providers to the detriment of implementing the IPv6, for example, may cause serious damage to network development. Another risk is the emergence of an IPv4 black market, as a means of delaying migration, which may hinder control over the numerical uniqueness, in addition to complicating Internet operation.

8.4.2 Synchronization of network elements and the Brazilian Official Time

This topic addresses two simple and paramount issues that are still virtually unknown and often undervalued: synchronization of network elements and the Brazilian Official Time.

There are usually detailed records (known as logs) on the operation and actions carried out by devices comprised in the Internet infrastructure, such as servers and routers. When cross-referenced, these logs play a key role in trouble-shooting technical issues, security incidents and even cyber crimes. Hence, their time coding must be very accurate and precise. In other words, Internet devices may be set to the right time, which enables several Internet applications to work properly and applies to all devices connected to the network.

Since computers and other devices are not able to adjust their time alone, these must be synchronized with an external reference. This is the purpose of the NTP.br (Network Time Protocol), a joint initiative between the NIC.br and the National

Observatory (ON) to provide time reference on the Internet. This is synchronized to the Brazilian Official Time and to the world UTC standard and is free of charge. As part of the same initiative, a website was created and promotional actions are carried out, such as lectures in universities and technical events. Hence, the NTP.br may be deemed a structuring project that helps improving the operation of the Internet infrastructure and making it safer, and its use in Brazilian networks is expressly recommended by the CGI.br.[174]

In 2011, the agreement between the NIC.br and the ON was renewed for 05 more years. A banner in the shape of a working clock was also created, which may be integrated to any website to provide the right time to users; enabling them to know if their PC is set to the right time and post the result on twitter to promote the NTP.br. Furthermore, cryptography features have been implemented to the system and the whole content of the website was revised.

8.4.3 Internet Exchange – PTTMetro

One of the most important initiatives of the NIC.br is PTTMetro.[175] It consists of a structuring project aimed at creating Internet Exchange Points (IXP) across Brazil. IXPs are components of the Internet infrastructure that enable direct interconnections between several networks in a restricted geographic area (usually a city or conurbation), enabling networks to exchange traffic between them.

There are several advantages to centralized direct connections between networks: smaller networks and providers save money, because they can exchange traffic directly with their peers and no longer have to pay upstream agents, direct connections mean faster speeds and an overall more resilient network, and local traffic is dealt with locally. An example of a potentially problematic situation that is eliminated by this initiative is when a citizen depends on a packet traveling long distances, often to foreign countries, to access its council's website, when the council is just next door. This happens because the citizen and the council are connected to different Internet providers. IXPs, therefore, improve the Internet structure in the country, in addition to making it cheaper, more reliable and faster for all.

---

[174] The CGI.br recommended that Brazilian networks use the NTP, through Resolution 009/2008, following instructions on the website: <www.ntp.br>. Accessed on 20.07.12.

[175] Traffic charts are available at: <http://www.ptt.br>. Accessed on 15.08.12.

The PTTMetro initiative aggregates the role of fostering and creating new IXPs across the country (when there are favorable technical conditions for it) and of operating them providing a high quality service. The organization in charge of investing in equipment and operating IXPs is the NIC.br, which usually relies on the support of other institutions for investments in dead fiber optics and datacenters. Several existing IXPs result from the cooperation between the RNP (National Research Network) and the NIC.br. In 2011, there were IXPs in several places in the country and the total aggregate traffic was approximately 100 Gbps.

PTTMetro is the fastest growing IXP in the world. It is a member of the Euro-IX, European Associations of IXPs, which is currently expanding its global operations, in addition to being one of the founder members of the newly created LACIX, Latin American and Caribbean Internet Exchange Point Association.

8.4.4 Network Quality Assessment

Another area of operation of the NIC.br is Internet quality assessment; its complexity and relevance are often underestimated. That is because the quality of the Internet cannot be assessed by simply creating a website to measure the download speed experienced by users. In fact, the National Broadband Plan, which we discussed in Topic 8.1 of this publication, states that because broadband speed is not a consensual criterion, it is not a good indicator of the quality of the Internet.[176]

Hence, assessing Internet quality requires more than just measuring bandwidth. Other important factors must also be taken into account, such as respecting the principle of network neutrality (discussed in Topic 3 of this publication), preventing traffic shaping, which prioritizes some types of applications over other, or even respect and full implementation of the DNS protocol.

In 2011, initiatives to assess the quality of the Internet in Brazil were structured in three main stages:

---

[176] Page 24 of the PNBL states that "the existing definitions of broadband are always based on download speed, but there is no consensus as to what this speed might be. This may be explained by (i) how difficult it is to set forth traffic standards that reflect the diversity of expectations, behaviors and standards of end users and (ii) the explosive increase in traffic, which render obsolete any definition based only on the bandwidth of access to the Internet, thus requiring constant updating." Hence why the Plan's definition does not use numbers, but whether the bandwidth available meets the demands of society at that particular moment in time. Available at: <http://www.google.com.br/url?sa=t&rct=j&q=plano%20nacional%20de%20banda%20larga%20pdf&source=web&cd=3&ved=0CGYQFjAC&url=http%3A%2F%2Fwww.governoeletronico.gov.br%2Fanexos%2Fplano-nacional-de-banda-larga%2Fdownload&ei=SI4IUPPfJ4GS9gTp8MShBA&usg=AFQjCNHK78IA39qh-TjnwT92Ngk9yM-IBQ>. Accessed on 19.07.12.

- International connectivity;
- Brazilian backbone and backhaul; and
- Last mile (connection to users).

This year the NIC.br has been involved in the international projects TTM (Test Traffic Measurements, from the European Regional Registrar) and SIMON (the Monitoring System of the LACNIC, the Latin American and Caribbean Regional Registrar). It also implemented the SAMAS (Automatic System for Autonomous System Measuring) to measure the quality of the national backbone and backhaul, and used the SIMET (Last Mile Traffic Measuring System) to measure the quality of connectivity for users. In particular, the SIMET operated with two versions, a simplified one with Web tests, and a more comprehensive one, with dedicated hardware developed by the organization, as part of a pilot project in partnership with INMETRO, Anatel and other collaborators.

8.4.5 Cert.br

One of the missions of the CGI.br is to coordinate and integrate all Internet service initiatives in Brazil, promoting technical quality, innovation and widespread service availability. In this context, its noteworthy activities include promoting studies and recommending procedures, technical and operating rules and standards for network security and Internet services, as well as for its increasing and adequate use by society.

Such activities are carried out under the scope of the Brazilian Network Information Center (NIC.br) and the Brazilian National Computer Emergency Response Team (Cert.br). As we'll see in more detail below, these organizations carry out several activities with the strategic objective of increasing security levels and incident response capacity in networks connected to the Internet in Brazil. The Cert.br's operation focuses on raising awareness of security issues, analyzing trends, assessing the correlation between events in the Brazilian Internet and supporting the creation of new CSIRTs (Computer Emergency Response Groups) in Brazil.[177]

[177] Information on CSIRTs in Brazil may be found at the website <http://www.cert.br/csirts/brasil/>. Accessed on 15.08.12.

Security Incidents

In regards to security incident handling, the Cert.br is in charge of notifying, overseeing and supporting the incident response process and, when needed, connecting the parties involved. As part of these activities, it (i) supports the attack recovery and assessment process for compromised systems, (ii) collaborates with other organizations, such as other CSIRTs, companies, universities, Internet access and services providers and backbones, and (iii) stores public statistics of incidents managed and spam complaints received.

Fighting spam

Reducing the amount of spam in Brazil requires a series of actions, including policies implementation by Telecoms Operators and access and service providers, such as Port 25 management, recommended by Resolution CGI.br/RES/2009/001/P of the Brazilian Internet Steering Committee, as well as raising users' awareness of the need to have a proactive stance on the Internet.

In order to foster the implementation of measures by different sectors of society, in 2011, debates with broadband network operators and Internet access providers were intensified to promote adoption of good practices to reduce spam coming from Brazilian networks. The main focus was the implementation of Port 25 management. Meetings were promoted by the CT-Spam, and the Cert.br attended the debates and helped preparing materials. In November, 2011, a Cooperation Agreement was entered into by Anatel, the CGI.br, the National Union of Telephony and Mobile and Personal Services Companies (SindiTelebrasil) and the Internet Access and Services Providers Association, supported by the Attorney General's Office and Consumer Protection agencies, to implement Port 25 Management.

Training and raising awareness

The following activities are carried out to increase the number of trained professionals and to raise national awareness of Internet security issues:

Material Preparation

Preparing documents and materials to raise awareness among Internet users:

- InternetSegura.br – redesigning the InternetSegura.br portal to turn it into a focal point for initiatives related to raising awareness of security issues. NGOs, companies and organizations are able to contribute by describing their institutional projects on the topic.
- New version of the Internet Security Handbook – in 2011 the Cert.br worked on creating a new version of its Internet Security Handbook. This new version, to be launched in the first half of 2012, will be illustrated and include specific sections on privacy, social networks and mobile technologies.

Licensed Courses from the *Carnegie Mellon University*

Training courses on security incident management, particularly for CSIRTs (Computer Security and Incident Response Teams) and institutions that need support to create their own CSIRTs.

The following courses are offered from the CERT® Program, of the SEI/CMU and licensed by the Cert.br:

- *Fundamentals of Incident Handling*
- *Overview of Creating and Managing CSIRTs*
- *Advanced Incident Handling for Technical Staff*

Trends Analysis

HoneyTARG Project

In 2011, the Cert.br restructured its Trends Analysis and Attack Monitoring Projects to gather exclusively domestic efforts and efforts involving international partners under the same umbrella.

In September, 2011, the Chapter "honeyTARG Chapter" (http://honeytarg.cert.br/), overseen by the Cert.br, officially became part of the "Honeynet Project" (http://www.honeynet.org/). This Chapter is comprised of 2 Projects that use low interactivity

honeypots to detect malicious activities that abuse the Internet infrastructure, namely: the "Distributed Honeypots Project" and the "SpamPots Project"

Distributed Honeypots Project

This project has become part of the daily routine of the Cert.br and it is a thermometer of malicious activities in the Brazilian Internet space. Malicious activities detected by the sensors also enable detecting compromised Brazilian devices. Network administrators are notified when a series of malicious activities are observed originating in their networks.

The project also continues to send IP address data related to attacks on honeypots to the following National CERTs: ArCERT (Argentina), AusCERT (Australia), CERT Colômbia (Colombia), JPCERT/CC (Japan), CERT-Polska (Poland), CERT.PT (Portugal) Q-CERT (Qatar), CERT-TCC (Tunisia) and CSIRT Antel (Uruguay). Furthermore, data is sent to the organizations that maintain these projects to alert administrators of attacks coming from their networks: Team Cymru, Active Threat Level Analysis System (ATLAS) Project and Shadowserver Foundation.

SpamPots Project

The goal of this project is to use low interactivity honeypots to obtain data related to Internet infrastructure abuse for spamming. We currently have sensors in partnership with the following institutions (in order of sensor activation): CSIRT USP (Brazil), CERT.at (Austria), CSIRT Antel (Uruguay), SURFnet (Holland), TWCERT (Taiwan), CLCERT (Chile), AusCERT (Australia) and CSIRT UTPL (Ecuador). There is also a sensor maintained by the Cert.br itself.

The work in partnership with the team of the e-SPEED lab, from the DCC/UFMG, also continued to improve data mining algorithms and to determine better analysis and data reporting processes. In 2011, the scope of the survey was expanded to intensify efforts towards detecting botnets and phishing campaigns.

The academic results of the survey so far have been published in related scientific conferences:

- Spam detection using web page content: a new battleground – Ribeiro M. T. C.; Teixeira L. V.; Veloso A. A.; Guedes Neto D. O.; Meira Junior, W. ; Chaves M. H.; Steding-Jessen K.; Hoepers C.. In: The 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference (CEAS 2011),

2011, Perth, Australia. Proc. of The 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference, 2011. p. 83-91.

- Detecção de Spams Utilizando Conteúdo Web Associado a Mensagens – Ribeiro, M. T., Teixeira, L. V., Guerra, P. H. C., Veloso, A., Meira Jr., W., Guedes, D., Hoepers, C., Steding-Jessen, K., Chaves, M. In: XXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2011), 2011, Campo Grande. Anais do XXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2011). SBC, 2011. p.455 – 468
- SpSb: um ambiente seguro para o estudo de *spambots* – Silva, G. C. ; Arantes, A. C. ; Steding-Jessen, K. ; Hoepers, C. ; Chaves, M. ; Meira Jr., W. ; Guedes, D.. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2011, Brasília. Anais do XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2011. p. 1-5.
- Fatores que afetam o comportamento de spammers na rede – Silva, G. C. ; Steding-Jessen, K. ; Hoepers, C. ; Chaves, M. ; Meira Jr., W. ; Guedes, D.. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2011, Brasília. Anais do XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2011. p. 1-14.

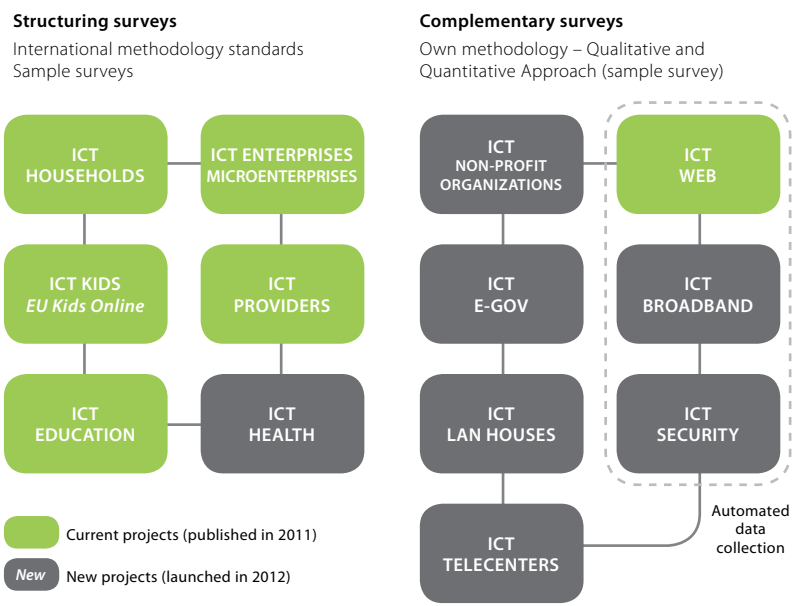
8.4.6 CGI.br / NIC.br surveys and analyzes on the use of ICT in Brazil

Within the scope of its mission to coordinate and integrate all Internet service initiative in Brazil, promoting technical quality and widespread availability of the services on offer, one of the noteworthy roles of the Brazilian Internet Steering Committee (CGI.br) is: promoting specialized research on the use of information and communication technologies (ICT). Hence, the CGI.br, through the Brazilian Network Information Center (NIC.br) and its Center of Studies on Information and Communication Technologies (Cetic.br), since 2005, has been carrying out surveys to produce indicators and statistics on the progress of the Internet in several sectors of the Brazilian society.

Since its inception, the Cetic.br has been observing the debate surrounding digital inclusion in the country: public and private sectors' approaches have been marked by great transformation potential and promises to enable public policies and/or national development programs to promote social and economic transformation. Indicators and statistics produced by the Cetic.br contribute

consistently not only to produce relevant information on the development of the use of the network in the country, but also, and more importantly, to the analysis of its impacts on the Brazilian socioeconomic development resulting from the national debate regarding digital inclusion. Over the years, the Cetic.br has consolidated its position as a reference center for the production of indicators and statistics on the use of information and communication technologies and, more importantly, on the use of the Internet in Brazil. The Cetic.br has been concentrating its efforts on broadening the scope and improving the quality of the indicators and statistics produced annually in its surveys. These efforts aim to ensure reliability of the results, to produce higher quality information and, most importantly, higher degree of international comparability. This includes employing qualitative and quantitative research methodologies, based on international reference models, such as the methodological references and data collection instruments determined by the UN's Partnership on Measuring ICT for Development, as well as Eurostat, Unesco, OECD and UNCTAD documents.

The aim of this document is to synthesize the main research projects conducted by the Cetic.br to measure the use of ICTs in several sectors of society: ICT Households, ICT Kids, ICT Enterprises, ICT Education, ICT Providers, ICT Electronic Government, ICT LAN Houses, ICT Telecenters, ICT Non-profit Organizations, ICT Web, ICT Health, ICT Broadband and ICT Accessibility. The figure below shows a summary of all the CGI.br's research projects currently being carried out by the Cetic.br.



ICT Households Project

The ICT Households Survey, in its 7th edition in 2011, is aimed at outlining a comprehensive picture of ownership and use of information and communication technologies in Brazil. The methodological procedures of the ICT Households survey are based on the guidelines of the Organization for Economic Cooperation and Development (OECD), of the Statistical Office of the European Commission (Eurostat), and the Observatory for the Information Society in Latin America and the Caribbean (Osilac), of The UN's Economic Commission for Latin America (ECLA).

The sample plan of the survey is designed based on the parameters set forth by the National Households Sample Survey (PNAD) – conducted annually by the Brazilian Institute of Geography and Statistics (IBGE) -, in order to ensure representativeness of the Brazilian population aged over 10 years old. The sample comprises 25,000 households spread country wide and includes urban and rural areas. The survey uses in-person or face-to-face interviews guided by structured questionnaires for data collection. The modules for which indicators have been produced are:

- Module A – Access to Information and Communication Technologies;
- Module B – Use of computers;
- Module C – Internet use;
- Module G – Electronic Government;
- Module H – Electronic Commerce;
- Module I – ICT Skills
- Module J – Wireless Access (mobile phone use);
- Module K – Intention to purchase ICT equipment and services.

ICT Kids Project

The aim of the ICT Kids Survey is to comprehensively map out ownership and use of information and communication technologies in Brazil by the new generations of kids aged 5 to 9. It is based on the ICT Households questionnaire, which, in turn, is based on the methodological standards of the Organization for Economic Cooperation and Development (OECD) and the Statistical Office of the European Union (Eurostat).

In order to ensure that the Brazilian population is accurately represented, the regional, economic and social diversity of the country has been reproduced in the sample design through quotas for specific variables. Hence, the sample in the ICT survey is systematic, stratified by conglomerates and quotas in the last stage.

Interviews regarding the main households sample were conducted in person in 2,516 households, with individuals aged between 5 and 9 years old. The survey enables results to be presented according the following intercrossing variables: geographic region, social class, family income, level of education, age group, gender and employment status. The field study used structured questionnaires in face-to-face interviews at interviewees' households. Interviews were conducted in the presence of children's parents and/or guardians. The modules for which indicators have been produced are:

- Module A – Access to Information and Communication Technologies in the household;
- Module B – Use of computers;
- Module C – Internet use;
- Module E – Use of e-Mail;
- Module I – ICT Skills; and
- Module J – Use of Mobile Phones.

ICT Enterprises Project

The ICT Enterprises Survey, in its 7th edition in 2011, aims to outline the use of ICTs by businesses, including differences between industries, sizes (number of employees) and the five regions of the country.

The survey universe comprises companies with 10 or more employees, from 11 segments of the UNCTAD's ISIC classification. Rais is used as the base-record for sample design and for the selection of companies to be interviewed. The choice of ISIC segments, as well as the company sizing structure, was based on international guidelines to ensure that data are comparable. Interviews with enterprises were conducted over the phone, based on structured questionnaires, with average duration of 30 minutes. The aim of the survey was to interview the person in charge of the computing, IT, computer network management areas or

equivalent department. What's more, in companies with 250 or more employees, part of the questionnaire was applied to an employee of the financial, accounting or administrative departments. The modules for which indicators have been produced are:

- Module A – General Information on ICT Systems;
- Module B – Use of the Internet;
- Module C – Electronic Government (e-Gov);
- Module E – Electronic Commerce;
- Module F – ICT Skills; and
- Module G – Software.

ICT Education Project

The revolution caused by Information and Communication Technologies (ICTs) has been causing profound changes in all segments of society, including in education. The use of ICTs in educational systems has become a challenge and a priority in many countries, which have been investing on the use of new technologies in education. Implementation of technological infrastructure – i.e. desktop computers, laptops, TV sets, camcorders, etc. –, teacher training and creation of e-learning content are a few examples of these investments.

The ICT Education Survey aims to determine how computers and the Internet are incorporated and sued in Brazilian public schools through teaching practices and school management. Furthermore, it aims to provide supporting information for the design of actions and policies for the incorporation of ICTs in schools. The survey sample has 700 schools -500 of which are public primary and secondary schools and 200 of which are private- in urban areas across the national territory. The following have been excluded from the sample draw: rural areas, federal schools and classes with more than one grade;

The survey requires data collection from players in the education system – i.e. principals, directors of studies, teachers (Portuguese and math) and students (5th year of Elementary School I, 9th year of Elementary School II and 2nd year of Secondary School). In-person (face-to-face) interviews using structured questionnaires were used for data collection. The modules for which indicators have been produced are:

- Module A – Profile (Principals, Directors of Studies, Teachers, Students);
- Module B – Outline of Computer and Internet Use (Principals, Directors of Studies, Teachers, Students);
- Module C1 – Administrative activities, planning and interaction with the community (Principals);
- Module C2 – Planning activities (Directors of Studies);
- Module C3 – Educational and school activities (Teachers);
- Module C4 – School activities on the Internet (Students);
- Module D – Computer and Internet Skills (Teachers and students);
- Module E – Specific training (Teachers and Students);
- Module F – ICT Infrastructure in schools (Principal);
- Module G – Barriers preventing use (Principals, Directors of Studies and Teachers).

ICT Providers Project

The progress of digital inclusion in Brazil is directly dependent upon the development and expansion of the Internet infrastructure, particularly in less attractive markets. Internet Service Providers (ISP), which comprise access, content, hosting, e-mail or application providers, are key players in the expansion of the network infrastructure in the country. In this context, effective inclusion of Brazilian citizens in the digital world is dependent on the presence of Internet access providers in small municipalities in the countryside of Brazil.

The ICT Providers survey was designed by the Brazilian Internet Steering Committee (CGI.br) and the Brazilian Network Information Center (NIC.br) to produce a comprehensive overview of the Internet access provision market in Brazil, by creating a National Registry of Providers. This survey was supported by the following Providers Associations: ABRANET, ABRAMULTI, ABRAPPIT, ABRINT, ANID, Global Info, Internet Sul and Rede TeleSul. The modules for which indicators have been produced are:

- Module A – General Features of the services provided;
- Module B – Internet connection infrastructure;
- Module C – Business Information (customers, market, speeds offered).

ICT Electronic Government Project

In line with several governments worldwide, which incorporate information and communication technologies as tools to modernize public administration and to improve efficiency, quality and transparency of the public services provided, the Brazilian government has also been investing on expanding electronic government programs (e-Gov). However, to ensure public managers are able to strategically plan e-Gov services that meet the needs of individuals and enterprises, they require structured and systematic information on the use of the e-Gov in Brazil.

The ICT Electronic Government Survey aims to produce indicators and statistics on the use of the e-Gov in Brazil. The methodology consisted of two different approaches: a qualitative approach, which was based on focal groups with citizens and in-depth interviews with businesses; and a quantitative approach, through a sample survey and structured questionnaires. Data collection for the quantitative survey was conducted with businesses and citizens nationwide. In the qualitative approach, the aim was to capture key emerging issues from the information provided by interviewees, and the meanings attributed to them, based on the assumption of a subjective and socially constructed scenario. The modules for which indicators have been produced are:

- Module A – Internet Use;
- Module B – Use of Public Services over the Internet;
- Module C – Perceptions about the Electronic Government;
- Module D – Barriers preventing the use of the Electronic Government;
- Module E – Government-Society Communication; and
- Module F – Context Variables.

ICT LAN Houses Project

LAN houses create opportunities for citizens to engage in society and to browse through the world of culture, education and entertainment, through information and communication technologies. Among other issues, the low penetration of Internet access in low income households has created the ideal environment for the establishment and expansion of businesses offering such services. In 2007 the CGI.br emphasized the phenomenon of LAN houses, evidencing the issue of local access, as they survey revealed that most Brazilian Internet users in urban areas had accessed the service from paid public centers. The ICT LAN Houses represents an unprecedented initiative by the CGI.br, outlining business management issues, the infrastructure available, customer profile and the profile of entrepreneurs.

The ICT LAN Houses Survey aims to produce an overview of LAN House management in Brazil, and it may be sectioned in three broader themes: the first is related to the dimension of the sector: the number of LAN houses in the country, their location, and the variables affecting their presence. The second theme is related to the profile of these businesses – i.e. outlining these businesses regarding their infrastructure, business model, sustainability, among other indicators. The third theme is related to identifying alternatives for the future of this segment, based on changes in the Brazilian access profile.

For the purpose of this survey, an LAN house is defined any commercial establishment providing access to computers and Internet services, even if such services are not its main business purpose. The survey uses a probability sample, stratified in stages, using area sampling and probability proportional to size (PPS) to select municipalities and census sectors. Interviews are carried out in person, face-to-face, using structured questionnaires, with the owner or manager of the business. The modules for which indicators have been produced are:

- Module A – Facility Infrastructure
- Module B – Business Model
- Module C – Sustainability
- Module D – Software;
- Module E – Future Investments;
- Module F – Management Tools;

- Module G – Customers' Profile; and
- Module H – Managers' Profile.

ICT Telecenters Project

Telecenters are key facilities in the digital inclusion process. In addition to providing computers connected to the Internet, telecenters offer an opportunity for citizens to access, use and take ownership of digital technologies for problem solving and citizenship. Without veering far from digital inclusion, telecenters can play several roles, such as providing an open space for training and qualification, with document processing and printing resources, as well as other computing resources. As free facilities they are able to meet the demands of several population profiles across the country, including areas outside the scope of the market.

The goal of the ICT Telecenters survey is to assess the contribution of federal public policies – i.e. GESAC, Telecentros.BR, Community Telecenters – to digital inclusion in Brazil. The specific goals of the survey are:

- To determine the working condition of telecenters.
- To determine critical factors for the effective operation of telecenters.
- To assess how telecenters contribute to promoting digital inclusion.
- To research the socioeconomic impacts and outcomes of implementing a telecenter in a local community.
- To determine criteria for prioritization in telecenter deployment.
- To suggest improvements for public policies for digital inclusion.
- To develop a methodology that can be duplicated.

The target population of the survey is telecenters, which are defined as any organization that has received any type of benefit from the Ministry of Communications to set up a facility to provide the population with free access to computers connected to the Internet.

ICT Non-Profit Organizations Project

The primary objective of the ICT Non-Profit Organizations Survey is to map out the ICT infrastructure, uses and capabilities/skills of non-profit organizations;

producing data to assess the penetration of these technologies, the resources available to manage these institutions and the potential benefits for their respective communities. The survey's goals may be grouped into three wider topics:

- Determining the ICT infrastructure of non-profit organizations;
- Understanding how ICTs are effectively used by non-profit organizations, based on aspects such as resource prospecting, management, use of the Internet's social networks, mobilization and communication;
- Assessing the information and communication technology capabilities/ skills accrued by institutions, as reflected by its leaders' and collaborators' ability to use such technologies innovatively.

ICT Web Project

Since mid-90s the Brazilian Web has been expanding profusely, both in number of users and in the range of services and application on offer. Its increased used by the Brazilian population is evident: from 37 million users in 2005 it has grown to 65 million users in 2009. No less impressive is the change in the behavior of individuals using an increasing number of transaction services in virtual environments, as shown by the CGI.br's surveys.

The impact of the use of the Web and the Internet on society, individuals and organizations has become the objective of research, not only in the specialized fields of applied computing, but also in organizational and sociological studies. As an essentially dynamic and limitless network, both physically and virtually, our knowledge of the Internet must be comprehensive, to ensure it transforms freely and is available, reliable and accessible to all.

Hence, the Brazilian Internet Steering Committee – CGI.br and the Brazilian Network Information Center – NIC.br, through the W3C Brazil and the Center of Study and Research in Network Technology and Operations – Ceptro.br, have designed another initiative to produced further knowledge and understanding of the Brazilian Internet: the Web.br Census Project. Conducted in partnership with the Logistics and Information Technology Bureau from the Ministry of Planning, Budget and Management (SLTI / MPOG), the Brazilian Association of State Bodies for Information and Communication Technologies (ABEP) and the National Institute of Web Science and Technology (inWeb), as well

as the methodological support of the Center of Studies on Information and Communication Technologies – Cetic.br, this project aims to produce indicators on the progress of the Brazilian Web, as explained in further detailed below.

The .gov.br Census Project

This research project is an initial effort towards determining the methodology required to estimate the so-called "coverage status", in order to produce more accurate estimates of the size of the .gov.br. Its goal was to estimate the share of the Web.br corresponding to the .gov.br domain, and then survey the information available using automated data collection techniques from .gov.br pages.

Data collection in governmental domains found 18,796 websites under the .gov.br domain, based on the URLs searched. Determination of the overall number of websites began with the analysis of data from the following sources:

- Domains identified as .gov.br (domains exclusive to the federal government). The list of these domains was provided by the Brazilian domain name registry authority, Registro.br, instructed by the Ministry of Planning, which is in charge of the use of domains under the .gov.br domains.
- Domains identified under the acronym -uf,gov.br, registered by state data processing companies, related to state governments;
- Results of consultations and information searches, using search engines, to complement previous information.

These different sources were consolidated and used as basis for an automated collection system. This compilation was aimed at producing a registry that could include the largest possible number of governmental websites and webpages, in order to make it as close as possible to a census of the Brazilian governmental Web.

The ICT WEB Survey aims to reproduce the .gov.br study to all existing .com.br. domains. Due to the size of the .com.br WEB and the time, processing, connectivity and disk resources required to collect, store and process these data, we've chosen to design a sampling technique for the WEB. This project is still under development.

ICT Health Project

Based on the assumption that ICTs can contribute to the design of public policies in several health-related areas, the ICT Health 2012 survey aims to investigate the following:

- Mapping out the ICT infrastructure available at Brazilian health facilities (hospitals, clinics, outpatient services, etc.)
- Mapping out ICT-based applications that support medical services and facility management.
- Investigating the activities carried out using ICTs and the skills of the professionals in charge of them.
- Understanding the motivations and barriers for the use of ICTs by healthcare professionals (managers and healthcare providers).
- Creating a historic series of data to support public policy design, implementation and assessment.

ICT Broadband Project

The Brazilian Internet scenario is currently marked by increasing installed fixed broadband access points: 15.5 million in 2010, according to data from Anatel (National Telecommunications Agency). However, broadband services are provided primarily to higher earning households (Classes A and B), in the most economically viable urban areas of the country. This shows that digital inclusion, more importantly the universalization of broadband access in the country, is a challenge.

On the other hand, many of those who already have fixed broadband access are not happy with the services contracted. The main complaints filed by consumers in consumer protection agencies are related to the high cost of the service, the lack of technical viability to install the service and the quality of the service disruptions and instability).

The ICT Broadband survey overall is aimed at assessing the quality of fixed broadband services in Brazilian households from a panel sample over a period of six months to a year. The results of the survey reveal, for example, if the service provided by Broadband Internet providers is compliant what has been contracted by consumers. Furthermore, the survey maps out broadband access

in Brazil, identifying potential bottlenecks and priority areas, thus serving as potential basis for public policies for Internet universalization. The methodology employed in the survey is quantitative, with a longitudinal approach, using a panel of households with broadband connections.

ICT Accessibility Project

The ICT Accessibility Survey is aimed at investigating the barriers preventing digital inclusion and impairing the more effective use of networks by all Brazilian citizens, focusing particularly on disabled individuals. Initially, an exploratory study was conducted on the use of the Internet by different target audiences, this aimed to identify accessibility challenges to universalizing the Internet and the Web. The specific objectives of this survey are:

- To identify the main uses of the Internet by people with eye, hearing and physical disabilities; kids and computer/Internet users;
- To assess the benefits of the Internet as perceived by the target audiences surveyed;
- To determine how learning takes place using the Internet;
- To determine the use, availability and means of access to aid technologies;
- To identify the obstacles and barriers preventing effective use of the Internet by people with disabilities; kids and computer/Internet users.

8.4.7 The Web As Seen by W3C Brazil

The Internet and the Web are not synonymous. The World Wide Web, or simply the Web, is the best known means for accessing the information provided by the Internet. The Web is a set of services that allows one to open documents located anywhere in the world via hyperlinks, browse sites with a wide variety of content, and interact in social networks. Thus, the Web uses the Internet as a means, but does not use the Internet itself. Technically, the Internet is a networked infrastructure globally connecting devices that use TCP/IP to communicate with each other, and the Web is an application that uses the Internet to share digital objects – videos, images, effects.

The Web serves to expose, reference, and link in a digital network. Observing the Web means tracking how and under what conditions it fulfills its role

and the factors that have appeared as obstacles to the Web achieving its full potential.

The World Wide Web Consortium (W3C)[178] is an international consortium in which member organizations, a full-time staff, and the general public work together to develop standards for the Web. Led by Web inventor Tim Berners-Lee and CEO Jeffrey Jaffe, the W3C's mission is to direct the World Wide Web to achieve its full potential through developing protocols and guidelines that ensure its long-term growth.

The Web's social value lies in the new possibilities for human communication, commerce, and knowledge sharing. One of the primary goals of the W3C is to make these benefits available to all people, regardless of their hardware, software, network infrastructure, language, culture, geographical location, or physical and mental capacity.

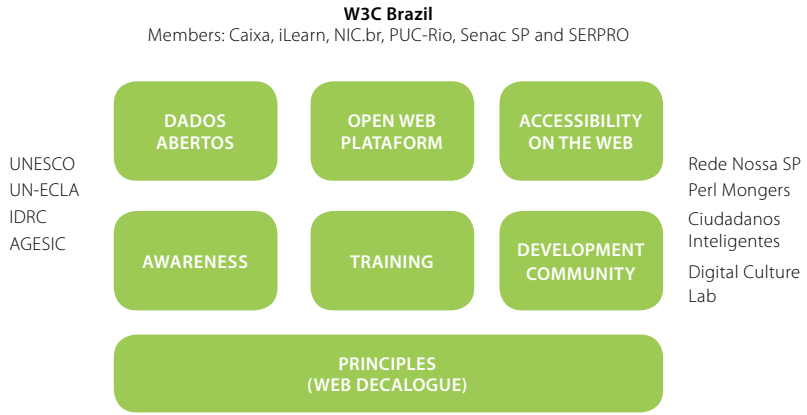
The number of different types of devices that can access the Web grows every day. Everything from cell phones, smartphones, PDAs, interactive TV systems, voice command systems, kiosks, and even some appliances can access the Web. The W3C's vision for the Web presupposes participation and knowledge sharing to build trust on a global scale.

The Brazilian office of the W3C is hosted by the Brazilian Internet Steering Committee (CGI.br), whose objectives are to coordinate and integrate all Internet service initiatives in the country, promoting technical quality, innovation, and dissemination of services offered. To perform these activities, CGI.br established a civil, non-profit organization called the Brazilian Network Information Center (NIC.br).

[178] Available at: <http://www.w3.org/>.

Based on these principles, W3C Brazil developed the "Brazilian Web Decalogue"[179]: Web for all, Web in everything, Web organized by standards, accessible Web, reliable Web, Web with multiple authors and readers, Web to serve democracy, Web for socio-economic development, Web that preserves its memory, and Web by all.

In 2011, the W3C Brazil, using the "Brazilian Web Decalogue", focused on three areas of activity, which generated several products in 2012: Open Web Platform, Web Access and Open Data. The W3C Brazil has six affiliate members – Box, iLearn, NIC.br, PUC-Rio, Senac-SP, and SERPRO. It also has national partners such as the Brazilian Association of Research Institutes (ABEP), the Office of the Controller General, the State of São Paulo, the State of Rio Grande do Sul, the Brazilian Digital Culture Laboratory, the Ministry of Planning, Perl Mongers, and Rede Nossa São Paulo, as well as international partners such as the Uruguayan Agency for the Development of e-Government and the Information Society – AGESIC, Chile's Ciudadano Inteligente, the UN Economic Commission for Latin America and the Caribbean – ECLAC, UNESCO and IDRC Canada (see below).



Source: W3C Brazil Office

[179] Brazilian Web Decalogue available at: <http://www.w3c.br/decalogo/>.

Accessibility on the Web

Accessibility on the Web means permitting and promoting access for people with disabilities to the Web. According to the IBGE 2010 Census, 24% of the population (45,623,910 people) suffers some type of disability. Of these disabilities, most are related to visual impairment: 35,791,488 people with some type of sight problem (this includes the 528,624 blind people).

The W3C established the Web Content Accessibility Guidelines – WCAG[180], international guidelines for creating accessible web pages that guide developers to code their pages so they do not create barriers to access for people with disabilities. According to data from the 2010 Dimensions and Characteristics of the Brazilian Web[181] survey dimensions and characteristics of the Brazilian Web: a study by the gov.br, only 2% of Brazilian government pages were accessible. In the following year, the same survey showed an increase in this number, which jumped to 5%. It is still a low number, but a significant jump indicating that web accessibility is beginning to be taken into consideration in Web projects in the ".gov.br" domain.

Since the inauguration of the W3C Brazil office, the institution has promoted activities to foster and broaden the discussion of Web accessibility in Brazil. By August 2012 there had been more than 40 lectures in Brazil and abroad disseminating standards for a more accessible Web.

Since 2009, W3C Brazil has promoted activities on December 3rd, proclaimed by the UN as the International Day of Persons with Disabilities. Every year on this day, the W3C Brazil website undergoes interventions to remind people of the importance of Web accessibility.[182] There are three types of pages, three types of navigation experience: a completely black page, one in which only keyboard buttons function (the mouse is deactivated), and one which uses extremely large font sizes. This initiative shows that it is easy develop a Web page that meets accessibility criteria.

In 2011, W3C Brazil launched the National Award for Web Accessibility – Todos@ Web, to reward people and companies that have developed important Web

[180] Available at: <http://www.w3.org/TR/WCAG/>.

[181] Available at: <http://www.cgi.br/publicacoes/pesquisas/govbr/>.

[182] Available at: <http://w3c.br/3-dezembro/>.

accessibility initiatives: websites that properly follow the standards and are accessible to people with disabilities and innovative assistive technologies so that people with disabilities may have autonomy in Web access. The winners of the first year's awards were divulged in June 2012 in a grand ceremony that took place at the São Paulo Inclusion Memorial and was attended by over 300 people.[183]

Open Data

Open data means the availability of information represented in open and accessible format so they can be reused and/or combined with information from other sources to generate new meanings. More specifically, they are computer data in such a format that they may be accessed by other computers via the Internet to produce applications and information from the processing and transformation of the original data, whether combined or not with other data from other computers.

Globally, the W3C has produced technologies and standards that enable the publication and reuse of data in open format. As these technologies and standards are in open format with free licenses, they may be used freely by anyone.

However, the production, processing, publishing, and reuse of open data are no small tasks. Although it is not difficult, the work requires technical expertise, attention to processes and legal aspects, and a technological infrastructure that is simple, stable, and scalable.

W3C Brazil has developed a series of activities to promote the consistent and ongoing implementation of open data by organizations and the development of a consistent public policy on the subject.

In 2011, W3C Brazil published manuals for different publics interested in the subject. The *Open Data Manual – Government*[184], a translation with additions of the Open Knowledge Foundation's *Open Data Manual*. It was the first manual in Portuguese on the subject and sought to delineate the concepts and best practices for public administrators. The second manual, *The Open Data Manual*

[183] Available at: <http://premio.w3c.br/>.

[184] Available at: <http://www.w3c.br/Cursos/CursoDadosAbertos>.

– *Developers*[185], presented to the Web development community how to publish and reuse data in an open format.

A consistent open data project presupposes the participation of technicians who know the open standards for data formatting and, if possible, the vocabularies and ontologies. W3C Brazil offered two courses on *How to Publish Open Data*[186] and *Basic and Advanced Aspects of Engineering Ontologies* for Brazilian government technicians with the aim to support the development of the National Open Data Infrastructure (INDA), in coordination with the Ministry of Planning.

The amount of government data with potential for being published in open format is immense, as are demands for information by civil society. The optimal point between supply and demand is when supply and demand coincide. For this reason, W3C Brazil created an Open Data Working Group bringing together various public agencies with public-interest data and civil society organizations seeking government data to improve their activities. In 2011, this group established a consensus on 10 priorities that define the areas in which existing data are highly important and can be made available. The goal is to create at least two open-format databases by the end of 2012.

As a result of these actions, governments are beginning to publish their data in open format. The Government of the State of São Paulo increased the number of available open-databases. The Brazilian House of Representatives provides an API (Application Programming Interface) for data access. The Court of Accounts of the State of Ceará also publishes budget data for the state's municipalities.

Another result of W3C Brazil activities in this area is the international repercussion and the invitation to join a Latin American initiative to promote open data as public policy. The Open Data for Latin America and the Caribbean – OD4D project began in the second half of 2011 and offered a seminar in Rio de Janeiro for different countries in the region – the first of its kind on this subject in Latin America.

A particularly special consequence for W3C Brazil was the sanctioning of the Access to Information Act by president Dilma Rousseff. It addressed not only information access as a guaranteed right, but also included an article requiring that information be published on websites and that such sites enable

[185] Available at: <http://www.w3c.br/pub/Materiais/PublicacoesW3C/manual_dados_abertos_desenvolvedores_Web.pdf>.

[186] Available at: <http://www.w3c.br/cursos/dados-abertos/saopaulo-2010-06/>.

automated access by external systems in open, structured, and machine-readable formats. The result of a joint effort by W3C Brazil and many other organizations that supported the drafting of the final text, the new law opens enormous possibilities for growth in the use of open data from the moment it enters effect in 2012.

The Open Web Platform

The Open Web Platform is a set of technologies developed by the World Wide Web Consortium, jointly with other partners, which was defined in 2011 by W3C CEO Jeff Jaffe, as "a platform for innovation, consolidation, and cost efficiencies" for the Internet.

This collection of technologies consists of code and specifications developed within Working Groups hosted and promoted by the W3C. There are more than 500 individuals who participate in these working groups and come from affiliated organizations belonging to the consortium. In addition more than 100 professionals work full time on developing a Web for all.

Together with other W3C initiatives, such as Open Data and the Decalogue itself, the Open Web Platform allows Web interfaces access to interoperable interfaces with linked content that is classified to facilitate searches, providing users with a more complete Web experience.

The consortium's *modus operandi* focuses on producing components for Open Source components to allow its implementation without cost or licensing fees. The Platform's main goals are:

- To promote the Semantic Web
- To facilitate offline access
- Access via different devices
- To promote improved connectivity for better communication
- To improve integration, experience and performance of applications and web content
- To offer accessible and rich effects and interactions via CSS3

Below there is a small overview of some technologies that, over the past two years, have been recommended by the W3C to build an Open Web. Adherence

to recommended standards is directly proportional to the quality of services, considering that it allows Web use to achieve its full potential.

HTML5: is the fifth version of HTML, which is the markup language used to enable browsers to interpret content. HTML5 aims to present multimedia content in a more accessible and integrated manner, as well as improve consistency so machines may better understand content.

CSS3: is the newest version of CSS, which applies styles to HTML pages. CSS3 presents new possibilities for the Web because it allows for rich interaction effects such as animations and transitions.

SVG: is a vector graphics language for describing drawings and images – i.e.: SVG allows machines to read image content different from the contents of JPEG or PNG images, for example. It also allows for enlarging images without losing quality. SVG is the only open format and was created by the W3C in 1998.

WAI-ARIA: (Web Accessibility Initiative – Accessible Rich Internet Applications) is a set of W3C recommendations for accessibility in rich interactions.

MathML: is a recommendation for representing symbols and mathematical formulas. It was created by the W3C Math Working Group.

WebGL: (Web Graphics Library) is an API for JavaScript (ECMAScript-based language) that enables rendering 2D and 3D elements using the HTML5 canvas element.

Web Storage: are recommendations and protocols for storing data in a browser – similar to cookies, but without storing the information in the HTTP request header. This means better data security and compliance.

Indexed Database: is a recommended standard for storing data input by the user. For example, it allows different browsers to have access to specific customizations such as bookmarks.

WebSocket API: is a protocol that allows for updating in real time, overcoming the limitations of the HTTP protocol. It is an effort to provide applications with zero latency connectivity between clients and Web servers.

Geolocation: is a recommendation to provide the location of any real-world object on the Web.

Over the past two years W3C Brazil has been promoting the Open Web Platform among the Web developer community. It offered courses in HTML5[187] and CSS3[188] training many market professionals, particularly those related to training institutions, in order to spread knowledge. To reinforce course learning, it created a thread[189] on HTML5 that brought together not only former students of the courses but also others interested in the topic.

Although the Open Web Platform has not been established yet as an official W3C standard (many modules of HTML5 and CSS3 are still in the testing phase) it has become a *de facto* standard. In Brazil, large corporations have already started to make their content available in HTML5 (e.g. Folha de S. Paulo and Globo.com), recognizing the value that this platform has to offer.

In conclusion, we can see, little by little the Brazilian Web is organizing according to standards, and these are increasingly for open access and interoperability. However, it is not immune to the market-locked dispute between an open Web for all and closed apps platforms – especially on mobile devices – that imprison users and put up barriers to the free exchange of content. Smartphones stores and apps cannot be referenced (e.g. linked or marked as favorites on email or Twitter) because they are out of the Web

We must be increasingly attentive. As Tim Berners-Lee said, "The Web is critical not merely to the digital revolution but to our continued prosperity – and even our liberty. Like democracy itself, it needs defending".[190]

[187] Available at: <http://www.w3c.br/Cursos/CursoHTML5>.

[188] Available at: <http://www.w3c.br/Cursos/CursoCSS3>.

[189] Available at: <https://mail.nic.br/mailman/listinfo/w3c_html5>.

[190] Article by Tim Berners-Lee for Scientific American Brazil. Available at: <http://www2.uol.com.br/sciam/reportagens/vida_longa_a_web.html>.

9

Relevant Debates in Other Countries

9.1 United States of America

9.1.1 SOPA and PIPA

SOPA (*Stop Online Piracy Act*) and PIPA (*Protect Intellectual Property Act*) are two American bills that aim to regulate the contents available on the Internet to protect intellectual property rights and to fight online piracy.

SOPA was presented by the president of the House of Representatives' Judiciary Committee, Lamar Smith, Texas, on October 26, 2011. Its aim is to increase the American government's ability to deal with copyrights breaches in the digital environment, in addition to preventing exchange of protected materials between Internet users. According to the bill's preamble, it aims "To promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property, and for other purposes".

Basically, the act targets online transfer of copyrights protected works against criminal laws, traffic of hazardous goods or services and intellectual property rights protection. Furthermore, it gives the Attorney General powers to protect American consumers and to prevent the U.S. from supporting infringing foreign websites. It also foresees a system to prevent American funding of websites

dedicated to stealing American property and grants immunity to service providers who voluntarily take action against such websites and against websites that threaten public health.[191]

The PIPA, also known as Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act. It was introduced by senator Patrick Leahy, on May 12, 2011, and it is a re-write of the Combating Online Infringement and Counterfeits Act (COICA), rejected by the Parliament in 2010. Similarly to SOPA, the Protect IP Act is aimed at "preventing online threats to economic creativity and theft of intellectual property, and for other purposes".[192]

This act aims to create additional legal resources against websites registered and operated abroad, in addition to curbing financial incentives to intellectual property theft and regulating voluntary actions against websites that are stealing American intellectual property.[193]

Although both bills are aimed at stopping illegal downloading and other forms of web piracy, by establishing systems for removing websites that the Department of Justice deems that are "dedicated to infringing activities," there are significant differences between them. While SOPA's provisions would extend to any website committing or facilitating copyright infringement, PIPA would only extend to websites with no significant use other than copyright infringement.[194] For example, the first could affect websites such as blogs, social networks, video and e-mail providers, search engines, etc.; whereas the latter would only affect copyrights infringing file sharing websites.

Their provisions also differ in implementation. SOPA requires search engines to remove infringing websites from their indexes, which is not foreseen by PIPA. Furthermore, PIPA requires more court intervention to take down a website, which may be viewed as positive; but, it has no provisions to penalize a copyrights holder for making a knowingly false claim of infringement.[195] On the

---

[191] Concepts extracted from the Headers of the SOPA bill.

[192] Text extracted from the introduction to the PIPA bill.

[193] Concepts extracted from the Headers of the PIPA bill.

[194] *SOPA and PIPA Bills: Differences Between the Two Internet Privacy Acts*, International Business Times: <http://www.ibtimes.com/articles/283906/20120118/sopa-pipa-bills-differences-internet-privacy-senate.htm>. Accessed on 14.02.12.

[195] *What's the difference between SOPA and PIPA?*, Social Media Collective Research Blog: <http://socialmediacollective.org/2012/01/17/whats-the-difference-between-sopa-and-pipa/>. Accessed on 14.02.12.

other hand, SOPA has a provision for such cases that makes copyrights holders liable for damages and legal costs.

9.1.1.1 Criticism against SOPA and PIPA

The media, institutions and society extensively criticized both bills at the end of 2011 and start of 2012, mostly indiscriminately due to the similarities between the two. In this context, two organizations played a prominent role, namely the EFF (Electronic Frontier Foundation) – American institution that protects rights in the digital world -, by frequently taking a stance on its website, through several articles analyzing the bills and their repercussions, and Google, which organized an online petition[196] against the bills.

Generally, all criticisms were based on two pillars: potential threats to copyrights and the innovation potential of society through the Internet. Critics to the bills were almost unanimous in claiming that the project will lead to global censorship on the Web, as they grant the U.S. government the right to take down content based on vague terms, in addition to granting immunity to Internet providers for arbitrarily blocking entire websites, without the requirement for a court ruling.

Several aspects of these bills have become prominent. The first of these is the issue of civil liability for Web content. According to the bills, websites in general (from magazines, video and music portals and social networks) would be co-liable for posting or duplicating infringing links. Several websites have areas for comments, such as blogs, newspapers, etc., and even if links are posted on such areas, websites will still be held liable. An aggravating factor is the collaborative nature of websites that are enabled by users' contributions, which means that the content is not moderated, such as social networks, microblogs or video portals. These websites, therefore, would be very likely to be taken down, if they didn't implement their own control of the content being posted, which defeats the purpose of such websites in the first place.

It is noteworthy that Internet providers and companies responsible for websites, in order to prevent litigation in U.S. courts against the government, would be practically obliged to monitor their users. This would be an additional task for

[196] Available at: <https://www.google.com/landing/takeaction/>. Accessed on 17.02.12.

the company, thus incurring in additional costs that would be higher the more threats to the website. Conveniently, the bills grant service providers immunity to voluntarily block any users or websites, with no need for a previous court order, if they believe these are infringing or causing infringement of copyrights. The only requirement is that they act "in good faith". Hence, corporations could create an arbitrary blacklist, with no legal legitimacy. This provision is criticized for creating an opportunity for abuse of power, in addition to punishing people who have not in any way breached any rights.

The fact that the law affects non-infringing individuals is one of the main concerns of the media. The Bills grant the Attorney General a series of powers and roles – the most extreme example of these would be the power to order the Judiciary to issue a court order for a website to be completely taken down, instead of just the infringing page, text or link. This both restricts the right to freedom of expression of those who are not infringing any intellectual property rights, and users' right to access the information contained in a particular website. Even the authors of the content posted on the website would be denied access to their creations. Alex Mcgillivray, general advisor to Twitter, gave his opinion on the topic in the blog Bricoleur, in a post called "Overbroad Censorship & Users".[197]

Another social sector negatively affected would be the international open software community which, according to the EFF[198], uses virtual private networks, proxies or private and anonymity software (Internet security software) to fight against authoritarian governments imposing direct censorship on the Internet. The Internet has increasingly been enabling social movements, as it promotes easy sharing of information and communication. Digital activists are renowned for using online tools in their fight for democracy in countries like China, Iran, Tunisia, etc. Such tools enable them to circumvent governments' attempts to block content on the Internet to reduce opposition to their policies and, often, these are somehow related to the U.S. through web hosting, financing mechanisms, etc. According to SOPA and PIPA, websites indicating how to circumvent their rules would be targeted by the government.

---

[197] Available at: <http://www.bricoleur.org/2011/12/overbroad-censorship-users.html>. Accessed on 17.02.12.

[198] Available at: <https://www.eff.org/deeplinks/2012/01/how-pipa-and-sopa-violate-white-house-principles-supporting-free-speech> e <https://www.eff.org/deeplinks/2011/11/hollywood-new-war-on-software-freedom-and-internet-innovation>. Accessed on 17.02.12.

As seen, unauthorized transfer of copyrights protected content would be targeted both by the Attorney General that would be entitled to take legal action, and by service providers, who would be at high risk of being held liable. For example, if someone posts a video of him/herself singing a copyrights protected song, this person could be jailed for up to 5 years; likewise, a video of yourself playing a video game, as a demo of how to progress on that particular game, would be taken down from the network. In this case the game developer would have to request banning of the video. If the website hosting the video failed to execute the request, causing re-notification, it could be entirely blocked until the issue had been resolved.

Infringing websites, in addition to the reproach to their content, would be subject to removal of their domain from search engine listings, if they failed to comply with court orders up to 5 days after receiving them. Furthermore, they would be prevented from receiving any online funding or remuneration. This would have a negative effect on payment service providers which, according to the bills, would become liable for preventing, forbidding or suspending their payment transaction services to infringing websites in the U.S. or under its jurisdiction. Internet advertisement services would also suffer, as they would not be allowed to advertise on infringing websites or post ads for such websites.

There is also an important concern in regards to the right to privacy, as American citizens' IPs could be screened for infringing content. Also, e-mail providers could block links in people's inboxes or on the body of e-mails.

Finally, the Bills do not only affect websites in the U.S. – there is an entire section on infringing foreign websites that are classified as such when they "infringe or promote infringement" of specific provisions of American laws related to copyrights and intellectual property rights. Providers will have up to 5 days to implement technical measures to prevent access by users located in the U.S. to the infringing content, if required by a court order. Lawsuits are filed by the Attorney General, who'll decide if a website in infringing copyrights or intellectual property rights.

News indicates that organizations constantly targeted by piracy activities stand to benefit from these bills, such as content producers (film and music industries), TV broadcasters and game developers.

9.1.1.2 Blackout

The opposition against the American anti-piracy bills, SOPA and PIPA, had enormous repercussion, particularly in the digital environment, resulting in the biggest online protest in history. On January 18, 2012, there was a planned blackout on the network, when websites were voluntarily taken down, making their content fully or partially unavailable or displaying protests on their home pages. The movement attracted more attention when the network giants, such as Wikipedia, Google, Reddit, Wordpress, among others, joined the protest, which led to the cancellation of the impending vote on the Bills.

According to data from the website Fight for the Future, one of the main activist groups involved in the SOPA Strike, in excess of 115,000 websites took part in the blackout and approximately 4 million e-mails were sent to the American Parliament.[199] Furthermore, elected American representatives received around 8 million calls from members of society criticizing the bills – another way of taking a stance out of the digital world.

Google played a key role in the fight against SOPA and PIPA. Together with AOL, Ebay, Facebook, Twitter, Firefox, Linkedin and Zynga, it sent an open letter to protest against the bills highlighting the risks they would pose to innovation and job creation. Other letters were also sent by 17 founders of Internet companies, 39 law and public interest organizations, 41 human rights organizations, 110 law professors, 204 entrepreneurs. In excess of 113,000 people signed a petition sent to the White House refusing support to laws that violate freedom of expression, increase the risk to network security and compromise the dynamic and innovative nature of the global Internet.[200]

It is worth noting that protests and involvement in the blackout were not restricted to U.S. soil. People worldwide felt threatened by the bills which, albeit limited to American jurisdiction, affect global access to the Internet.[201] A website allegedly infringing anti-piracy laws could be blocked without a court

---

[199] Available at: <http://sopastrike.com/numbers/>. Accessed on 23.02.12.

[200] Data from Google's infochart available at: <https://www.google.com/landing/takeaction/>. Accessed on 23.02.12.

[201] Twitter, through a statement given by its CEO, acknowledged that the bills may not only affect American nationals. In his words: "it is foolish of us to shut-down a global business in response to single-issue national politics" (<http://www.portalmariana.org/internet/os-grandes-sites-da-internet-protestam-contra-os-projetos-de-leis-antipirataria-sopa-e-pipa/>. Accessed on 23.02.12.

order. In view of the fact that a lot of the world's Internet infrastructure is in U.S. soil, or is hosted by American platforms that allow indiscriminate access, people worldwide who access these websites for legitimate purposes – i.e. not related to piracy practices – on a daily basis would suffer. Hence, many critics of SOPA and PIPA claimed that these bills would jeopardize essential features of the network – i.e. universality and neutrality.

In Brazil, the following organizations helped plan the *blackout*: (i) the Mega Não! movement, which fights against vigilantism, threats to freedom on the Internet and network neutrality, (ii) Coletivo Trezentos, a blog that aims to emulate the collaborative nature of the Internet by having its content written by several authors, and (iii) Software Livre Brasil, a non-governmental initiative to foster sustainable production using new technologies, with high content and information sharing capacity. [202]

Institutions that took part on the blackout include, among others, The Brazilian Institute of Consumer Protection (IDEC) and all websites related to the Center for Technology and Society of the Law School of the Getúlio Vargas Foundation (CTS-FGV). The IDEC posted a message on its home page stating that "freedom and Internet users' rights worldwide are under threat." In line with the CTS-FGV, the institute also criticized the Brazilian counter part of SOPA and PIPA, known as the "Azeredo Bill", which aims to criminalize practices in the digital environment, including piracy. Hence, a campaign was created in 2011, named "Consumidores contra o PL Azeredo" ("Consumers Against the Azeredo Bill"), which collected 16 thousand signatures.[203]

The CTS-FGV, in turn, in partnership with the Ministry of Justice and in a largely collaborative online process, produced the Internet Regulatory Framework[204], i.e. the bill currently under assessment by the National Congress. According to Carlos Affonso de Souza, deputy coordinator of CTS-FGV, the Internet Regulatory Framework is regarded as an anti-SOPA bill, which, instead of

---

[202] Available at: <http://meganao.wordpress.com/o-mega-nao/o-que-combatemos/>. Accessed on 23.02.12.

[203] More information available at <http://www.oficinadanet.com.br/noticias_web/4815/no-brasil-idec-tambem-se-manifesta-contra-a-lei-antipirataria>. Accessed on 23.02.12.

[204] The legal document of the Internet Regulatory Framework resulted from a collaborative process, enabled by the online platform Cultura Digital (<http://culturadigital.br/marcocivil/>), and gathered comments from all sectors of society, submitted voluntarily and without moderation. To learn more about the project, see <http://www.nupef.org.br/sites/default/files/poliTICS_n%C2%BA7_1.pdf>. Accessed on 23.02.12.

criminalizing practices, reinstates principles that must permeate the network and protects basic rights in the digital environment.[205] "The CTS defends that intellectual rights protection must not supersede other basic rights, such as privacy, freedom of expression and, more importantly, access to knowledge and information".[206]

Some important personalities of the Internet world have also taken a stance against SOPA and PIPA. We may, for example, quote one of the founders of the worldwide web (www), Tim Berners-Lee, who says that the bills are against human rights: "If you're in America then you should go and call somebody or send an email to protest against these (censorship) bills because they have not been put together to respect human rights as is appropriate in a democratic country."[207] Vinton Cerf, one of the founders of the Internet, sent a protest letter to the author of SOPA, Lamar Smith, and to the members of the House's Judiciary Committee, in which he stated that "site blocking or redirection mechanisms are unlikely to make a significant dent in the availability of infringing material and counterfeits online."[208]

Protests were supported by the contrary statement issued by the Barack Obama administration against the American bill, in its official response to both petitions asking for the draft bills to be vetoed. The noticed, published on the White House blog, maintained that the important task of protecting intellectual property online must not threaten an open and innovative Internet.[209]

---

[205] This stance is discussed in the following articles: <http://www.info4.com.br/gomateria.asp?cod=600426&nome=1432&cliente=1432> and <http://oglobo.globo.com/tecnologia/artigo-discussao-da-sopa-ensaio-para-que-vira-no-futuro-3703202>. Accessed on 23.02.12.

[206] Available at: <http://direitorio.fgv.br/sopablackout>. Accessed on 23.02.12.

[207] Available at: < http://articles.businessinsider.com/2012-01-20/tech/30645823_1_human-rights-tim-berners-lee-sopa>. Accessed on 23.02.12.

[208] Available at: < http://www.examiner.com/internet-in-national/internet-founding-father-vinton-cerf-opposes-sopa>. Accessed on 24.02.12.

[209] Available at: < http://www.whitehouse.gov/blog/2012/01/13/obama-administration-responds-we-people-petitions-sopa-and-online-piracy>. Accessed on 24.02.12.

9.1.2 ACTA

9.1.2.1 Background

The Anti-Counterfeiting Trade Agreement (ACTA)[210] is a multinational treaty under negotiation for the purpose of establishing international standards for intellectual property rights enforcement and to aid the fight against infringing globally, through international cooperation. Originally created by the U.S. and Japan in 2006, since then the treaty has gained support from several countries worldwide, which were involved in the negotiations of the treaty and undersigned it in 2011.

The preamble of the treaty states the rationale for creating the ACTA. It states that effective enforcement of intellectual property rights is critical to sustaining economic growth. Hence, it aims to protect legitimate trade, right holders and legitimate businesses, as well as to curb organized crime.

The treaty foresees that each signatory country must provide adequate legal protection and effective legal remedies against intellectual property rights infringement; Civil judicial procedures to be made available to right holders must include injunctions, compensation paid by the accused to the right holder, as well as payment of profits from selling the unauthorized material and removing from circulation or destroying materials used to manufacture the infringing material. Judicial authorities may also have the power to order temporary measures to prevent infringement or to preserve evidence of the infringement.

In regards to border measures, the treaty excludes punishment for small quantities of goods of a non-commercial nature contained in travelers' personal luggage, with no definition for small quantities.

Criminal proceedings are only applicable to infringements in commercial scale (for economic advantage). These include criminal sanctions to infringing individuals or collective parties, at the signatory country's discretion, imprisonment, as well as monetary fines sufficiently high to provide a deterrent to future acts of infringement, seizure, forfeiture and destruction of goods.

[210] Its Portuguese version is available at: <http://register.consilium.europa.eu/pdf/pt/11/st12/st12196.pt11.pdf>. Accessed on 27.02.12.

The ACTA has a specific chapter on intellectual property rights enforcement in the digital environment. This chapter states that the parties agree to curb infringement of copyright or related rights over digital networks, and notes that enforcement procedure must preserve fundamental principles, such as freedom of expression, privacy and fair process; in addition to being implemented in a manner that avoids the creation of barriers to legitimate electronic commerce activity and competition. For that it uses terms like "adequate legal protection" and "effective legal remedies", but does not specify what these mean, only provides a rough idea of how to obtain them.

There is also an article on raising people's awareness. Hence, each signatory State shall "promote the adoption of measures to enhance public awareness of the importance of respecting intellectual property rights and the detrimental effects of intellectual property rights infringement."

9.1.2.2 Criticism from the opposition

Initially, ACTA negotiations were secret and only developed countries could take part.[211] The lack of more in-depth information on what was being discussed and awareness that the decisions on intellectual property rights would affect not only participants of the negotiations, abut also other countries not involved, including the societies of participating countries prompted the creation of a fiercely critical opposing movement. The EFF (Electronic Frontier Foundation) even claimed that civil society and developing countries were being internationally excluded from the negotiations.[212]

The population only became aware of what was being debated through documents leaked over the years, such as the "Discussion Paper on a Possible Anti-counterfeiting Trade Agreement" or negotiations reports. In May 2011, the official text of the treaty was published in English, French and Spanish. Many of the original concerns regarding previous versions of the ACTA had been

[211] André de Mello e Souza, in an article published on the Valor Econômico magazine and reproduced by the A2K project's blog, stated that "the lack of transparency in the negotiations is an attempt to avoid opposition from the international community and goes against the recent trend of multilateral forums enabling comments and intervention by non-governmental agencies, as well as of disclosing the preliminary text of agreements on the Internet." Available at: <http://www.a2kbrasil.org.br/wordpress/lang/pt-br/2010/09/o-acta-e-os-direitos-de-propriedade-intelectual/>. Accessed on 29.02.12.

[212] Available at: <https://www.eff.org/issues/acta>. Accessed on 29.02.12.

removed, which proves that the criticisms had an effect on the negotiations[213]. In October 2011, in addition to the U.S. and Japan, Canada, Australia, New Zealand, Singapore, Morocco and South Korea signed the treaty.

Also on the topic of how the ACTA developed, there has been intense criticism to the illegitimacy of the text. As a treaty, it is prepared by members of the Executive Authority of participating countries, thus not involving the Parliament.

In regards to the content of the treaty, opponents claim that it does not cover the physical versions of pirated goods, such as CDs and medications. Its scope even extends to the "middle-man" on the Internet, e.g. Internet service providers, as the ACTA, like SOPA and PIPA, enables signatory countries to hold these players liable for the actions of third parties on the network. Hence, they would be obliged to control the Internet and its users, which raises concerns for fundamental rights, such as privacy and freedom of expression, as well as fair use of copyrights. According to the same perspective, the ACTA would also limit creativity and innovation promoted by the collaborative features of the network.

Critics also target the process of determining the treaty's content by deeming it anti-democratic, as there was no transparency and the opinions of civil society groups, the general public, international institutions, such as the World Trade Organization (WTO) and the World Intellectual Property Organization (WIPO), and developing countries were not taken into account. As seen, none of these stakeholders had access to the content debated during negotiations until the official document was released in 2011, except through information leaked by sometimes unknown sources.

On the other hand, an advisory committee comprised by large American multinational corporations (members of the pharmaceutical and cultural production industries) was consulted during the draft stage and, as such, had access to its content. Moreover, the companies Google, eBay, Intel, Dell, News Corporation, Sony Pictures, Time Warner, and Verizon received a version of the draft treaty under a non-disclosure agreement.[214] According to the Brazilian Mega Não! movement, "lobbyists from large music, film, software, video games,

[213] Available at: <https://www.eff.org/deeplinks/2011/10/acta-signed-8-members-are-we-doomed-yet>. Accessed on 29.02.12.

[214] Available at: <http://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement>. Accessed on 24.02.12.

luxury goods and pharmaceutical companies had access to the preparatory documents for the ACTA and were able to influence negotiations".[215]

9.2 Spain

In a context where intellectual assets are strategic for companies and for the development and integration of the market economy, intellectual property rights play an important role, as they are viewed as the best mechanism for protection and fostering the development of new products and services – i.e. production and exploitation of intellectual content.

Technological development has multiplied and diversified how these assets are created, produced and exploited. In this context, current legal institutes face dilemmas and challenges to keep up and adapt to this new complex and dynamic reality enabled by the Internet. Nevertheless, this is not a new concern. Since 2001, Europe has been trying to adapt its common rules to the new economic reality and to the common market, with the European Parliament and Council's Directive 2001/29. This Directive is about harmonizing certain aspects of copyrights and related rights in the Information Society. As seen in the directive's recitals, the uncertainty created by new technologies has prompted a repressive response from several countries:

"Any harmonization of copyright and related rights must take as a basis a high level of protection, since such rights are crucial to intellectual creation. Their protection helps to ensure the maintenance and development of creativity in the interests of authors, performers, producers, consumers, culture, industry and the public at large. Intellectual property has therefore been recognized as an integral part of property."[216]

The French law, known as the Hadopi Law, is an extension of Directive 2001/29 EC and it includes the "three strikes and you're out" rule, which sets forth that if a user recurs in downloading unauthorized protected works, he/she will have his/her Internet connection blocked.

---

[215] Available at: <http://xocensura.wordpress.com/2008/09/22/o-silencio-sobre-o-acta/>. Accessed on 24.02.12.

[216] The full text of Directive 2001/29 EC is available at: <https://ciist.ist.utl.pt/docs_da/directiva_2001-29-CE.pdf>. Accessed on 20.07.12.

In 2011, however, Spain joined France in the group of countries that have adopted questionable measures to protect intellectual creations on the Internet. The Spanish government decided to introduce a provision in its Sustainable Economy Act (SEA). These additional provisions are based on the content of the Sinde Law, introduced in 2009, and largely criticized by the Spanish society, culminating with its veto at the time. It foresees the possibility of blocking Web pages that enable unauthorized downloading of files with copyrights protected content. When the provisions of the Sinde Law were presented in 2009, Wikileaks findings showed that pressures from the American and the Spanish governments had been the main drivers of the provision against downloading.

The Spanish Sustainable Economy Act (SEA) is the product of a legal initiative approved by the Spanish government, in 2009. Its main goal is to modernize the Spanish economy in the areas of finance, business and environment, in order to try to solve the economic crisis that has been burdening the country in recent years. The original version of the SEA contained the so-called Sinde Law – it was named after the Spanish minister of Culture, Angeles Gonzales-Sinde, who presented the law in response to a demand by the coalition of Content Creators and Industry, a pressure group comprised by the rights management society and societies that protect the interests of large companies.

The aim of the Sinde Law is to take down websites containing links for downloading copyrights protected content. From the outset, the Sinde Law raised several concerns related to breach of due legal proceedings, the right to privacy and freedom of expression.

According to documents disclosed by Wikileaks and published by the Spanish newspaper *El País*, the American government played a key part in hardening the Spanish copyrights law. In the referred article from 2008, the newspaper *El País* [217] revealed that the American government threatened to put Spain in its annual list of intellectual property enemies, prepared by the Chamber of Commerce and known as "Special 301", if the Spanish government failed to implement anti-piracy Internet policies. The American threats worked, as the Spanish government proposed the Sinde Law as part of its SEA, in 2009.

[217] Available at: <http://www.elpais.com/articulo/espana/EE/UU/ejecuto/plan/conseguir/ley/antidescargas/elpepuesp/20101203elpepunac_52/Tes>. Accessed on 20.07.12.

The procedure described by the law to take down websites begins with a notification by the copyrights holder to the Intellectual Property Commission (administrative body of the Ministry of Culture). Upon receipt of a notice, in order to obtain data such as the domain name owner, number of users of the website and other confidential data, the Commission must request a judge. The fact that a member of the Judiciary is involved from the start of the procedure is viewed as a means of ensuring fairness. However, this was not how the subject was viewed in 2009, when it was vetoed.

Perhaps because of Wikileaks' disclosures, which revealed the U.S. diplomatic scheming to influence the Spanish legal-cultural agenda, the Sinde Law was rejected by the Spanish Congress at first, by virtually all parties represented in the Congress – except for the Spanish Socialist Workers' Party (PSOE) -, according to the aforementioned article from the El País newspaper: [218]

For PP, the provision sought to "disguise," with a fast judicial proceeding, the fact that an administrative body, such as the Intellectual Property Commission, dependent on the Ministry of Culture, could take down websites. *"In practice, websites could be taken down without proper legal guarantees, which would open the door, from the political power, for breaching fundamental rights, such as freedom of expression," says José María Lasalle. Marta Gastón, speaker for the PSOE, countered that the legal system alone "may decide whether to close a website", and said that you can't "leave a sector that employs 800,000 people and accounts for 4% of GDP unprotected." She recalled that the Culture subcommittee agreed by majority to provide minimum guarantees for intellectual property protection, and said: "If we protect bricks more than ideas, we will be condemning our children to continue making bricks." (our highlights).*

As well as freedom of expression, another fundamental right would be directly affected by the Sinde Law, knowingly protection to private life, as it allows individuals who believe themselves victims of copyrights breaches to access users' personal data. A precedent in the Court of Justice of the European Union, actually involving Spain, has already rejected the possibility of Internet access providers taking action that puts private life in jeopardy to defend copyrights holders. In this context, the ruling on the Promusicae vs. Telefónica case

[218] Available at: <http://cultura.elpais.com/cultura/2010/12/21/actualidad/1292886001_850215.html>. Accessed on 20.07.12.

determined that intellectual property rights holders requesting personal data, such as the IP address, of individuals suspected of infringing their exclusivity rights, is against the fundamental rules of the European Union.

9.3 Switzerland

Unlike what happened in Spain (Topic 9.2), Switzerland decided not to change its internal legislation to include provisions for intellectual property rights protection in digital media, deeming their current legislation sufficient for that purpose.

The Federal Council of Switzerland was asked to position itself in relation to the topic and it prepared a report that was published in early December, 2011. The study assessed the possibility of legally restricting illegal downloads and existing measures in the international scenario to remedy the issue. The Swiss Government concluded that a new law or legislative reviews on the topic were not essential or even necessary at this time. On the other hand, it deemed necessary to monitor technological developments and the international debate on the topic to periodically reassess their stance and the need to adapt copyrights legislation.

In order to prepare this report, the Federal Council reviewed several international studies on downloading and sharing of music, films and games. A study titled "*Ups and Downs: The Economic and cultural effects of file sharing on music, film and games*",[219] commissioned by the Dutch Government in 2009, was used as reference by the Swiss government on piracy data. Increasing downloads and sharing of cultural assets has not affected people's intention to purchase other cultural assets, such as movies, theater and concert tickets. Even those who acquire their assets through downloads also buy them through traditional means, according to the Swiss government's report.

Three existing approaches to the topic in the international scenario have been highlighted. Each one of them was justifiably rejected, as summarized below:

[219] Available at: <http://www.tno.nl/content.cfm?context=thema&content=inno_publicatie&laag1=897&laag2=918&item_id=473&Taal=2>. Accessed on 20.07.12.

9.3.1 Progressive response or "three strikes and you're out" (French model – Hadopi)

Data disclosed by the French autarchy Hadopi, which aims to address creation on the Internet, revealed a drop in the number of illegal downloads and file sharing in France, in 2011. Although this result may be viewed as successful in reaching the autarchy's goals, the Swiss government believes that, from an objective perspective, a progressive response has long term consequences that are impossible to assess. As discussed in the government's report, it consists of a three-step mechanism of curbing practices, which progressively increases punishment for recurrence up to blocking connection.

The report also asserts that a progressive response requires implementation of a large State apparatus. On this perspective, the annual cost of operating Hadopi are estimated at 12 million Euros, according to the French public budget in 2011 for the Ministry of Culture and Communication. The Swiss government also questions the compatibility of progressive response mechanisms with International Conventions, particularly the report of the UN Human Rights Council, which established that blocking access to the Internet is against article 19, paragraph 3 of the International Covenant on Civil and Political Rights.

9.3.2 Filtering and blocking access to the Internet

The Swiss government's report indicates the importance of debating repressive measures, particularly those applicable to Internet access providers, as part of the network neutrality agenda. According to the counselors, this stems from the need to protect free competition and fundamental rights, such as freedom of expression, due legal proceeding and privacy. The same criticisms and limitations of the progressive response mechanism apply to filtering and blocking by access providers. Such measures are not compatible with the right to freedom of expression and the technologies used for filtering may seriously jeopardize privacy. Furthermore, the fact that blocking is not ordered by a legal authority, but by private companies, significantly increases the complexity of the issue and leads to debates on the role of the Judiciary in resolving issues that require remedies to damages incurred on the Internet.

9.3.3 Collective Licenses

Potential use of collective licenses for works disclosed on the Internet, for non-commercial purposes and combined with a remuneration system, is viewed as a feasible permissive approach. This solution would have the double advantage of legitimizing the biggest "downloaders", as well as remunerating uses such as streaming. However, according to the report, most of the Swiss population views this remuneration system as somewhat "unfair". This type of compensation would only be acceptable, if it took into account general fairness rules. Also, this regimen would need to be aligned with the international agreements signed by Switzerland. International Conventions, such as WIPO's, foresee it as an exclusive right of authors to disclose their works online. Exceptions and limitations to this right are only permitted in exceptional circumstances that do not hinder regular marketing of the work. In any case, rights holders are able to enter into agreements to achieve this, i.e. there is no need for a legal provision for it.

The Swiss government's report also questions the legitimacy of measures to curb copyrights infringements, stating that these should be applied within the limits of fundamental rights. It also asserts that several stakeholders view copyrights as an obstacle to accessing culture, and this line of thinking even had political support from the Swiss Pirate Party, which strongly opposed the idea of intellectual property as a means of fostering cultural production.

Despite criticisms of the unfairness of collective licenses, the Swiss government views an agreement between large media companies, collective management society and Internet access providers as desirable. However, by choosing a technically neutral regulation, the Swiss legislator has already legitimated the practices of Internet users by allowing them to copy files for personal purposes, regardless of whether the file source is infringing. Hence, the report concludes that there is no need for a specific law to regulate the illegal use of works on the Internet.